



情報セキュリティ教育

MicroWorld株式会社

（全従業員向け）

Vol.202109版

MicroWorld



当社の情報セキュリティ対策

- 当社では、情報セキュリティ対策の一環として、当社で業務にあたるすべての方に、情報セキュリティ教育を受けていただいております。

これから、ご説明する内容は、主に以下の事についてです。

- 機密情報漏洩防止
- 個人情報保護
- コンピュータウイルス対策
- 常駐先での注意点、等。
- テレワークでの注意点、等。

これらの内容は、非常に重要です。

情報セキュリティ違反がないように遵守して下さい。

個別事例に見る問題分析(1/2)

【事例1】

作業効率アップのため、**資料を自宅PCにダウンロードし作業**。数か月後、**PC ログのAI 分析で発覚**、情報漏洩として当事者に対して「即時退場」「取引停止」の措置をとった。また、未だに**本人の賠償リスク**は残っている。

論点

- いくら何か理由があっても、顧客情報漏えいに対する危機管理が、徹底されていたか？
- 業務PC上の操作は、メールタイトル、ブラウザ操作、Zipファイルの中身など、全部記録されているので、いつでも分析しているか？

【事例2】

入館カードを忘れ、同僚のカードを借りて入館。**違反行為**が発覚し、入館カードの貸借禁止のルールに反したため、借りた本人及び貸した同僚の**両名厳重注意処罰**。

論点

- 個人(機密)情報漏えいの危険性や、情報漏えいのリスクを、職員に徹底して教育していたのか？

個別事例に見る問題分析(2/2)

【事例3】

本人から在宅勤務の申告があったが、2時間後お客様から「連絡が取れなくて困っている」と問い合わせがあり、**実際には「寝ていた」**ことが発覚。

論点

- 勤務時間中に勤務をしているのか？
- テレワーク中に出勤時より綿密にハウレンソウをしたのか？

【事例4】

在宅勤務メインの者が出勤した際、他の同じ PJ メンバーは在席していなかったため、業務中に「**居眠り**」、「**スマホゲーム**」をそれぞれ実施。他 PJ の方から通報があり、後日その者達だと特定、発覚。両名に対して、**お客様から即時退場、会社として減給処罰**をそれぞれ科した。

論点

- 「一人のみ」の場合でもマナーを守り、勤務ができたか？
- 社会人として誤解されやすい行動はあったか？

セキュリティ事故が発生した場合

■ 信用失墜


- 取引先、顧客から信頼を失い、現在の契約が破棄される恐れがあります。
- また、顧客から当社との今後一切の取引が中止される可能性があります。

■ 被害額

- セキュリティ事故は毎年増加傾向にあり、被害額も増加傾向にあります。
- 個人情報漏洩による2009年に発生した想定損害賠償総額は、約3,890億円(約309億元)、1件あたりの被害額は、約2億6,683万円(約2,123万元)です。

■ 損害賠償

- セキュリティ事故が発生した場合、MicroWorld株式会社は、取引先から巨額の損害賠償を請求される可能性があります。
- ベースは、あなたの所属する会社に対して損害賠償請求を行います。
- あなたの所属する会社では、厳重注意、減給、停職、解雇、損害賠償等の処分を受ける可能性があります。



個人情報保護

■ 個人情報とは何か

- 個人情報とは、個人の氏名、住所、性別、生年月日、電話番号、Emailアドレスなど個人を特定できる情報のことを指します。
- 個人情報は、書類、データファイルの両方です。

■ 個人情報の取り扱い

- 業務で取り扱う個人情報は、業務上必要な場合のみの利用に限り、業務目的以外の利用、外部への持ち出しを一切禁止します。



書類、記録媒体の保管

■ 書類、記録媒体の放置禁止

- 離席時、机の上に書類、記録媒体を放置しないで下さい。
- 印刷後、プリンタ、複写機に書類を放置したままにしないで下さい。
- 業務終了後、書類、記録媒体は引き出し、書庫等に保管し施錠して下さい。

■ ホワイトボードの利用

- ホワイトボードは利用後、書き込みした内容を直ちに消去して下さい。



コンピュータウィルス対策


- ウィルス対策ソフトの導入、更新
 - 業務に使用するPCには、ウィルス対策ソフトをインストールします。
 - 常にウィルスパターンファイルを最新の状態に保つように更新して下さい。
- ウィルスチェック
 - 当社では業務に使用するPCは全て使用前にウィルスチェックを行います。
 - 業務開始後は、最新のパターンファイルで定期的にウィルスチェックを行って下さい。
- 不明なファイル
 - 送信元が不明なEmailアドレスからの添付ファイルは、絶対に開かないで下さい。
 - また、外部から持ち込まれた不明なファイルも絶対に開かないで下さい。
- 不正サイトへのアクセス禁止
 - ウィルス感染の恐れのある不正なサイトへのアクセスを禁止します。





不正ソフトウェアの利用禁止

- ファイル交換ソフトのインストール、利用禁止
 - Winny, LimeWire, Share, WinMX, XNap等のファイル交換ソフトのインストール、利用を禁止します。
- その他不正ソフトウェアのインストール、利用禁止
 - その他不正ソフトウェアや業務に無関係のソフトウェアのインストール、利用を禁止します。
 - 複数のコンピュータ上のデータ検索機能（例：Googleデスクトップ）等、PC内の情報を社外のサーバへ自動的に複製してしまう機能は、無効化してください。



遵守事項

（当社と取引先、常駐先での遵守事項）

- 当社規則、規程の遵守
 - 当社規則の、個人情報保護、機密情報漏洩防止対策の徹底、コンピュータウィルス対策は、必ず遵守してください。
- 取引先、常駐先の規則、規程の遵守
 - 当社の規則以外に取引先、常駐先ごとの規則、規程も、必ず遵守してください。

入館、退館時の注意事項

- 入館証は、常時見える位置に携帯して下さい。
- 許可された区域以外の場所は立入禁止です。
- 社内のエレベータ、社外、食堂等の共有スペースでは業務に関する話を禁止します。
- 業務契約終了後は、入館証、その他貸与品を当社或いは取引先に直ちに返還して下さい。
- 受託情報の廃棄・消去は下記の方法で行います。
 - 紙媒体・・・シュレッダーにかける
 - 電子媒体・・・ツールを用いて無意味なデータを上書きする
(メールデータも含む)
 - CD-R等書換え不可能な可搬記録媒体
・・・破壊する

PC管理 (1/2)

■ 個人のPCの持込、利用禁止

- 個人のPCは職場に持ち込み禁止とし、自宅でのテレワークのみ可能とする
- 業務には常駐先から貸与される業務用PC、もしくは、MicroWorld株式会社が所有する業務用PCを利用して下さい。
- MicroWorld株式会社から業務用PCを常駐先に持ち込む場合、必ずPC初期化、ウィルスチェック等を実施してから持ち込んでください。

■ ノートPC持ち出し禁止

- 原則、ノートPCの持ち出しを禁止します。
- 業務上、止む得ずノートPCを持ち出す場合、必ず部門責任者の許可を得て下さい。
- ノートPCを持ち出す場合、ノートPCは、常に携帯し、車内、バス、電車の網棚等に放置しないで下さい。

PC管理 (2/2)

- ノートPCのBIOSパスワード及びHDDパスワード
 - ノートPCには、必ずBIOSパスワード及びHDDパスワードを設定します。設定方法は、部門責任者或いは担当チームリーダーに確認して下さい。
- OSパスワードの設定
 - OSのパスワードを設定し、パスワードは他人に知られることのないように厳重に管理して下さい。
- ハードディスク暗号化ソフト
 - 顧客より要請がある場合、ハードディスク暗号化ソフトを利用してください。
- スクリーンロック(PC画面保護)
 - 離席する場合、コンピュータ画面をパスワードによりロックして下さい。
 - スクリーンセーバーによるパスワード保護は、5分以内に設定して下さい。
- ノートPCのワイヤーロック
 - 業務時間中、ワイヤーロックにより、ノートPCを机に固定します。
 - 業務終了後は、鍵の付いた机の引き出し、書庫等にノートPCを保管し施錠します。



電車の中等、社外での重要物の管理

- 重要物の入った鞆は、電車の網棚には乗せないでください。

お客様から受領した資料、お客様先入館証、本人の保険証やクレジットカードなどが入った鞆は、電車の網棚には乗せずに、自身の膝の上に置くか、しっかり手で持って保管してください。

- お客様の重要物を持って外出する際には、緊張感を持つようにしてください。

お客様から受領した重要物を持って外出する際は、常に注意して携帯し車内、バス、電車の網棚等に放置し、盗まれたり、失くしたりしないよう注意してください。



外部記録媒体の利用

■ 外部記録媒体の利用禁止

- 原則として、USBメモリ、CD-R、CD-R/W、DVD-R等の外部記録媒体の利用、持込、持ち出しを禁止します。
- 業務上、止むを得ず外部記録媒体を利用する場合、部門責任者の許可を得てから、当社或いは常駐先が提供する外部記録媒体を使用して下さい。使用終了後は、速やかに返却して下さい。
- 個人の外部記録媒体は、一切利用禁止です。
- 外部記録媒体を利用する際は、セキュリティロック機能のあるものを利用する、またはデータ暗号化による保護を行って下さい。



私的Email、私的Web閲覧禁止

- 私的Emailの利用
 - 業務に無関係の私的Emailの利用を禁止します。
- 私的Web閲覧
 - 業務に無関係の私的Web閲覧を禁止します。
- ネットワーク監視
 - ネットワークの利用状況は、当社或いは常駐先による監視がされています。私的Emailの利用、私的Web閲覧が発見された場合、処分される可能性があります。





情報セキュリティ違反

■ 注意、警告

- 担当者に対して、厳重な注意、警告を行います。
- チームリーダ、プロジェクト責任者は、情報セキュリティ違反がないよう、情報セキュリティ対策の周知徹底を行います。

■ 契約破棄、退場

- セキュリティ違反が改善されない場合、ベースは契約を破棄するものとし、担当者はプロジェクトから外れて頂きます。
- 重大なセキュリティ違反があった場合、ベースは契約を破棄するものとし、担当者はプロジェクトから外れて頂きます。



テレワークのご利用(1／3)

■ テレワーク作業可能場所

- 日本国内の届け済みの自宅
- 日本国内の出張時申請済み宿泊先
- 届け済みの会社事務所内

■ 誓約書

- テレワークルールを記載した誓約書に自ら署名し提出
- 誓約書はプロジェクト終了後も3年間保管する
- 許可された場所以外でのテレワークは実施しません
- 許可された以外の接続サービス以外は接続しません

テレワークのご利用(2／3)

■ 注意事項

- 毎日の出勤と退勤はリアルタイムで報告する
- 日報は退勤前に必ず提出すること
- 勤務時間中いつでも連絡が取れること
- 電話、メール、メッセージなどの返事が可能なことか、速やかに折返し返事すること
- 15分以上の離席はチームに連絡してから離席、戻ったら連絡すること
- Teams、Slackなど長時間操作がない場合、ステータスの変更があり、長い業務電話などにはご注意ください
- チーム内のコミュニケーションに努めること
- 家族・同居者など他人が見られないように注意すること



テレワークのご利用(3／3)

■ 禁止事項

- フリーなWIFI・不特定多数の人が利用するネットワークのテレワーク禁止
- 第三者の出入りを制限できない場所(カフェーなど)のテレワーク禁止
- 接続した端末に表示された内容を画面コピーもしくは撮影、録音すること禁止
- 許可された以外の接続サービス以外は接続しません
- 業務PCが常に監視されているので、中国語サイトなど業務と関係サイトのアクセス禁止
- 業務PCより外部への書き込み、アップロードは禁止



セキュリティ事故が発生した場合の対応

■ コンピュータウィルス感染

- ウィルスに感染した場合、或いはその恐れがある場合、直ちにコンピュータからLANケーブルを引き抜き、ネットワークから接続を切り離します。
- 直ちに上司、部門責任者に報告を行い、その指示に従って下さい。

■ 紛失・盗難

- 重要書類、データの入った外部記録媒体、ノートPCの紛失・盗難が発生した場合、直ちに上司、部門責任者に報告を行い、その指示に従って下さい。

■ その他

- その他のセキュリティ事故が発生した場合、セキュリティ事故を目撃した場合は、直ちに上司、部門責任者に報告を行って下さい。
- 自身のとるべき行動が分からない場合、自己判断せずに上司、部門責任者に尋ね、指示に従って下さい。

※上記等、事故が発生した場合、セキュリティ責任者に報告してください。

TISに常駐される方への注意(1/8)

TISに着任し業務開始までにしていただくこと

■ TISへ提出するもの／受取るもの

- ① **「誓約書」、「入館証等交付申請書」**を、提出します。「誓約書」は、内容を確認し、署名・捺印して、遵守事項は厳守してください。
- ② **「入館証」**を受取ります。

※入館証は担当部門より渡されます。これらは業務終了後帰任する際には、返却して下さい。なお忘れた場合、紛失・破損した場合は、速やかに担当部門へお問い合わせください。

■ 「情報セキュリティ講座」を受講してください

- **必ず**受講を完了してください。講座は規定や遵守事項を説明する「学習」と理解度を確認する「テスト」で構成されています。不明点があれば、担当部門の情報セキュリティ部門管理者へお問い合わせください。



TISに常駐される方への注意(2/8)

TISに着任し業務開始までにしていただくこと

■ PCの持ち込みについて

- 業務に必要なない資産や私物の持ち込みは「一切禁止」です。
- 業務完了後、持ち込みPCを持ち帰る場合、データの削除を行いますので、予めバックアップを取ることを推奨します。
- 持ち込みPCは、業務以外の用途で使用する事、指定LAN経由以外での接続やモバイルカード等による外部接続を禁止します。
- 持ち込みPCには指定の「ウィルス対策ソフト」「PC管理ソフトウェア」など(操作ログを記録されること)を導入します。
- メッセンジャーソフト、通信シミュレーションソフト、ファイル交換ソフトは使用禁止です。
- 業務上使用しているPC(持ち込みPC含む)を社外へ持ち出すことは「一切禁止」です。また社内ではセキュリティワイヤで固定し、鍵は情報セキュリティ部門責任者が保管することになっています。

TISに常駐される方への注意(3/8)

業務期間中、常に実施していただくこと

■ 常に実施すること

- 「ウィルス対策ソフト」は**最新状態で常時稼動**して下さい。
- **Windowsソフトに脆弱性が発見された場合、セキュリティパッチをあてる**依頼通知が管理部門より発行されますので、その場合は速やかに対応してください。

■ 電子メールの利用

- Emailで送受信された全ての情報は、機密情報として取り扱って下さい。
 - ① メール方法の徹底(送信は、許可するメール手段のみ使用可)
 - ② 本文には、機密事項を含めず、添付ファイルに記載し、添付ファイルは必ず暗号化すること。(開錠鍵は電話等で通知)
 - ③ メール送信先は、必要最低限とします。関係者全員をメーリングリストに登録し、送信する等、機密情報を散布するような行為は、情報セキュリティ上、行わないでください。
 - ④ 複数の相手先にメールを送信する際は、他のメールアドレスが表示されないように、メールアドレスをBCCにしてください。

TISに常駐される方への注意(4/8)

業務期間中、常に実施していただくこと

■ 情報の取扱い

- TIS及びTISのお客様の情報を業務遂行以外の目的で使用しないこと。
- 機密情報はTISもしくはTISのお客様に帰属します。業務終了後は全て返却してください。
- 「関係者外秘」「社外秘」を、開示範囲外の人に開示しないでください。
- 機密情報は使用后必ず施錠保管(引き出し・キャビネット)してください。
- 不審な電子メールは、受信しても廃棄してください。
- 機密情報(記録媒体・印刷物等)を机上に放置しないこと。PCにはスクリーンロックやPCロックをし、パスワードで画面を保護すること。
- 設計書、仕様書、委託業務に関わる全てのメール送受信文書は全部機密事項です。取扱いには、細心の注意を払うようにしてください。



TISに常駐される方への注意(5/8)

業務期間中、常に実施していただくこと

■ 報告事項

- ① ウィルスを検知したら、担当部門の情報セキュリティ部門管理者へただちに報告し指示を仰いでください。
- ② 情報資産の紛失、破壊、改ざん、漏えい等を発見もしくは疑いがある場合(入館証を紛失した場合等)等セキュリティ事故を発見したら、担当部門の情報セキュリティ部門管理者へ、ただちに報告し指示を仰いでください。
- ③ PCが盗難または紛失した場合、ただちにTISへ連絡してください。TISの委託業務終了後、委託業務に関する機密情報が保存されたPCの盗難、紛失の場合も同様です。PCの盗難は善管注意義務違反であり、実際に悪用が行われなくても、PCの管理者は責任を負わなければなりません。
- ④ メール受信文(添付ファイル)に個人情報と疑われる情報を発見した場合は、ただちに担当部門に連絡ください。

TISに常駐される方への注意(6/8)

業務期間中、常に実施していただくこと

■ 禁止事項

- ① 通常の業務で使用しているPCの持出は「一切禁止」です。業務上やむを得ずPCを持出す場合は担当部門責任者の許可を取り「持出専用PC」を利用してください。
- ② 機密情報の持出は原則禁止です。業務上必要な場合で担当部門責任者の許可がない限り、持出できません。
- ③ 携帯電話、電子手帳等へのメール送信は、禁止です。但し、パスワードロックされた機器に対してのみ、緊急時の連絡やスケジュールの連絡等業務に言及しない範囲でメールの送信を許可します。
- ④ TIS関連事業所内および、お客様事業所内でのWEBメールの使用は禁止です。
- ⑤ アカウントやパスワード等の認証情報、担当する業務に関する情報を第三者に教えないこと。

TISに常駐される方への注意(7/8)

業務期間中、常に実施していただくこと

■ 禁止事項

- ⑥ 担当する業務以外の情報にはアクセスしない。業務に無関係な情報や機能にアクセスしたり、情報の紛失、改ざん、破壊、漏えいしないこと。
- ⑦ 許可されていないデータ・機器・環境は使用しない。本番データをテスト用に使用しないこと。(自作データ又はスクランブル済のデータを使用すること)
- ⑧ 業務に必要なのない機器、記憶媒体、私物などの持込は一切禁止です。
- ⑨ 私用および不適切な電子メールや業務目的以外のインターネットの閲覧は禁止です。
- ⑩ 立入制限区域は、許可された人のみ入室が可能です。



TISに常駐される方への注意(8/8)

業務終了後、帰任前にしていただくこと

- TISへ返却するもの
 - 「入館証」を返却してください。
- 業務で使用したPCの情報消去
 - PCにダウンロードされた送受信メールと添付ファイルを削除します。
 - 使用したPCが、TIS以外の所有の場合、導入した「ウィルス対策ソフト」「PC管理ソフトウェア」「PCロックソフト」をアンインストールし、PC内の情報を消去します。





質問

- 不明な点があれば、質問して下さい。

MicroWorld





誓約書の記入

- 誓約書に記載された内容を理解した上で、誓約書に記入、署名して下さい。

MicroWorld

