文書番号：BSA-0018(7)
2022 年 1 月 20 日
東京 IT スクール事務局

東京ITスクール
TOKYO IT SCHOOL

東京 IT スクール Java 研修
セキュリティマニュアル 1.7 版

目次

東京ITスクール
TOKYO IT SCHOOL

1. 改訂履歴

版数	改版者	改版内容	承認者	承認日
1.7 版	山口	問合せ先電話番号の更新	宍戸	2022 年 1 月 20 日
1.6 版	鈴木	主に受講生用として改訂	藤井	
1.5 版	鈴木	自宅における PC の取り扱いの変更	藤井	2019 年 2 月 28 日
1.4 版	植木	作業場所における事故対応と報告の内容変更	宍戸	2017 年 6 月 20 日
1.3 版	植木	作業場所における書類、備品の取り扱い、作業場所における事故対応と報告の内容変更	宍戸	2016 年 12 月 1 日
1.2 版	植木	クリアデスクポリシーの内容変更	宍戸	2015 年 2 月 17 日
1.1 版	植木	東京 IT スクール事務局の連絡先変更、投稿メールのフォーマット追記	宍戸	2015 年 2 月 2 日
1.0 版	植木	PC のアカウントパスワードに関する追記、文書全体の文言修正	宍戸	2014 年 11 月 28 日
0.2 版	植木	立ち入り制限区域、入館証、自社との連絡方法、出欠管理表の管理方法、自宅学習、コンプライアンスに関する追記	宍戸	2014 年 11 月 6 日
0.1 版	植木	新規作成	宍戸	2014 年 11 月 6 日

2. 概要

1　はじめに

当マニュアルは受講生及びサポーター（社員及び外部講師）が、株式会社システムシェアード社内研修会場内及び社外研修会場内（以下作業場所と称する）において作業を実施するにあたり、遵守しなければならない情報セキュリティ項目について定めるものする。

2　管理体制

株式会社システムシェアード情報セキュリティ委員会の委員長を長とし、東京 IT スクール事務局を管理部門とする。事件、事故（以下インシデントと称する）発生時、サポーターは事務局へ速やかに報告をすること。ただし、インシデント内容により一時報告先の記載がある場合はそれに従うこととする。また、セキュリティに関する質問や意見があれば自由にメール投稿できるものとする。

東京 IT スクール事務局
TEL：03-3526-2490
mailto: edu@3sss.co.jp

件名：【セキュリティ】教室名_企業名_フルネーム_yyyyMMdd
内容：教室名、企業名、フルネーム、質問等を記載

なおメールアドレス等の受講生の個人情報は、研修以外の目的には一切使用しないものとする。

3. 個人情報、機密情報の取り扱いについて

1　個人情報及び機密情報の定義

当マニュアルにおける個人情報及び機密情報（以下秘密情報等と称する）の定義を以下に記す。

（1）個人情報
- 受講者及び所属する組織の登録情報、受講記録
- サポーター及び所属する組織の登録情報
- 個人を特定するに十分な項目の組み合わせ、国籍等機微な項目
  （例）当該情報に含まれる氏名、生年月日等により個人を識別することができるもの名簿等

（2）機密情報
- 研修の運用に関する情報
- その他、企業秘密に類する情報

2　秘密情報等の取り扱い

上記、秘密情報等の取り扱いについて記す。

（1）いかなる場合でも秘密情報等を構外へ持ち出したり、外部に漏洩したりしないこと
（2）秘密情報等を自宅で取り扱わないこと。ただし、講義資料等を除く。
（3）いかなる場合でも私有 PC、タブレット等を作業場所に持ちこないこと
（4）秘密情報等を私有 PC、タブレット等より取り扱わないこと
（5）記録メディアを作業場所に持ち込まないこと
（6）私有 PC であっても、ファイル交換ソフトウェアをインストールしないこと
（7）個人の履歴、機微な情報（精神、信条、罰則等）を話さないこと
（8）漏話の可能性がある秘密情報は閉域の場所へ移動すること
（9）slack での秘密情報等を含むファイルのやり取りは一切禁止とする
※秘密情報等を含まない一時的なものはやり取り可能
例：社名および氏名の記載された座席表 ×、ソースコードを記載した txt ファイル ○

4. 立ち入り制限区域について

作業場所への入退室に関して以下の物理的セキュリティ対策を施し、セキュリティレベルに応じた入退室管理を行う。作業場所におけるセキュリティレベルとその区域に関しては、研修会場内の掲示物を参照のこと。

1　株式会社システムシェアード社内研修会場内

	サポーター（社員）	サポーター（外部講師）	受講生
セキュリティレベル１	入室可	入室可	入室可
セキュリティレベル２	入館証着用時、入室可	入館証着用時、入室可	入館証着用時、入室可
セキュリティレベル３	入館証着用時、入室可	入室不可	入室不可
セキュリティレベル４	入室不可	入室不可	入室不可

（１）セキュリティレベル２の制限区域にサポーター、受講生以外が入室する場合は、その入退室に関する記録を取得し安全に管理するとともに、少なくとも１年間保管をする。
・入室者の氏名及び所属
・入室日時及び退室日時
・入室の目的
（２）セキュリティレベル２以上の制限区域に立ち入る全ての者に対して、入館証を着用すること。
（３）施錠出来る部屋が無人となる場合は施錠を行う。鍵は管理部が管理すること。

2　株式会社システムシェアード社外研修会場内

	サポーター（社員）	サポーター（外部講師）	受講生
セキュリティレベル１	入室可	入室可	入室可
セキュリティレベル２	入館証着用時、入室可	入館証着用時、入室可	入館証着用時、入室可

（１）セキュリティレベル２の制限区域は、囲い等で明示する。
（２）セキュリティレベル２の制限区域はサポーター、受講生、並びに企業関係者以外の入室を認めない。なお、入室する場合は入館証を着用すること。企業関係者が入室する場合はこの限りでない。
（３）施錠出来る部屋が無人となる場合は施錠を行う。鍵はサポーター（またはエリアマネージャー）が管理すること。

5. 作業研修場所における PC の取り扱いについて

機密情報等の漏洩を防ぐため、作業場所における PC の取り扱いを記す。

1　クリアスクリーンポリシー

（1）離席する場合は PC からログオフするか、パスワード付きでスクリーンをロックすること
（2）ホワイトボードへの板書は、作業終了後速やかに消去すること

2　ウィルス対策

（1）ウィルス対策ソフト
・ウィルス対策ソフトは常時起動しておくこと
・パターンファイルは自動的に更新される設定とする

（2）ウィルススキャン
セキュリティに対する意識付け、及び PC を保護するためウィルススキャンを実施する。

対象	受講生、サポーターが使用している PC
実施日	毎週水曜日の昼休憩時間
実施方法	別紙「PC セットアップマニュアル」参照

（3）PC でのインターネットの利用
・研修に関係のないサイトの閲覧は禁止とする
・FaceBook、Twitter 等インターネット上の SNS 利用を禁止する
・署名の無いあるいは信頼できない公開サイトの ActiveX や Java、JavaScript、VBScript 等のコードを実行しないこと
・Web メール、Dropbox、OneDrive、Google ドライブ等のサービスの利用は禁止とする
・ソフトウェアのダウンロード、インストールは禁止とする
・ダウンロードしても良いファイル形式は jpeg、png、gif 等の画像のみとするが肖像権、著作権の侵害に留意すること(JavaScript ライブラリに関してはサポーター(社員)が責任を持ってダウンロードし、ウィルススキャン実行後に配布等すること)

（4）PC へのデバイスの接続
・携帯電話、スマートフォン等を接続しないこと
・USB 接続によるデータ転送に限らず、充電も禁止とする

3　パスワードの取り扱い

PC の利用者はアカウントに紐付くパスワードの質を、次の通り維持すること。

（1）パスワードは秘密にしておくこと
（2）パスワードを記録した情報は、他人に見られない方法で保管し管理すること
（3）パスワードに対する危険の兆候が見られる場合は、パスワードを変更すること
（4）パスワードは質の良いものにすること
・パスワードは最短 8 文字とする
・パスワードは英大文字、英小文字、数字及び記号のうち、少なくとも 3 種類の文字列を混合させる
・類推可能なパスワード（誕生日、氏名等）にしない
（5）パスワードは毎月、定期的に変更すること
（6）LMS 等アクセス制御された Web サイト閲覧時に離席する場合は、必ず Web ブラウザを終了させるか、Windows のパスワード付スクリーンロックを実施すること
（7）LMS 等アクセス制御された Web サイトの閲覧において、他人のユーザ ID やパスワードなどを利用してアクセスしてはならない

6. 作業場所研修場所における書類、備品の取り扱いについて

1　クリアデスクポリシー

（1）作業及び研修終了後、机の上の整理整頓に努めること
（2）不要な LAN ケーブルは置かないこと
（3）清潔に保つこと

2　教室の鍵

教室の鍵、及びセキュリティカードはサポーター（またはエリアマネージャー）が管理し、解錠及び施錠はサポーター（またはエリアマネージャー）が行うこと。

3　書架の鍵

書架の鍵はサポーターが管理すること。また、スペアは東京 IT スクール事務局が管理すること。

4　移動中の注意事項

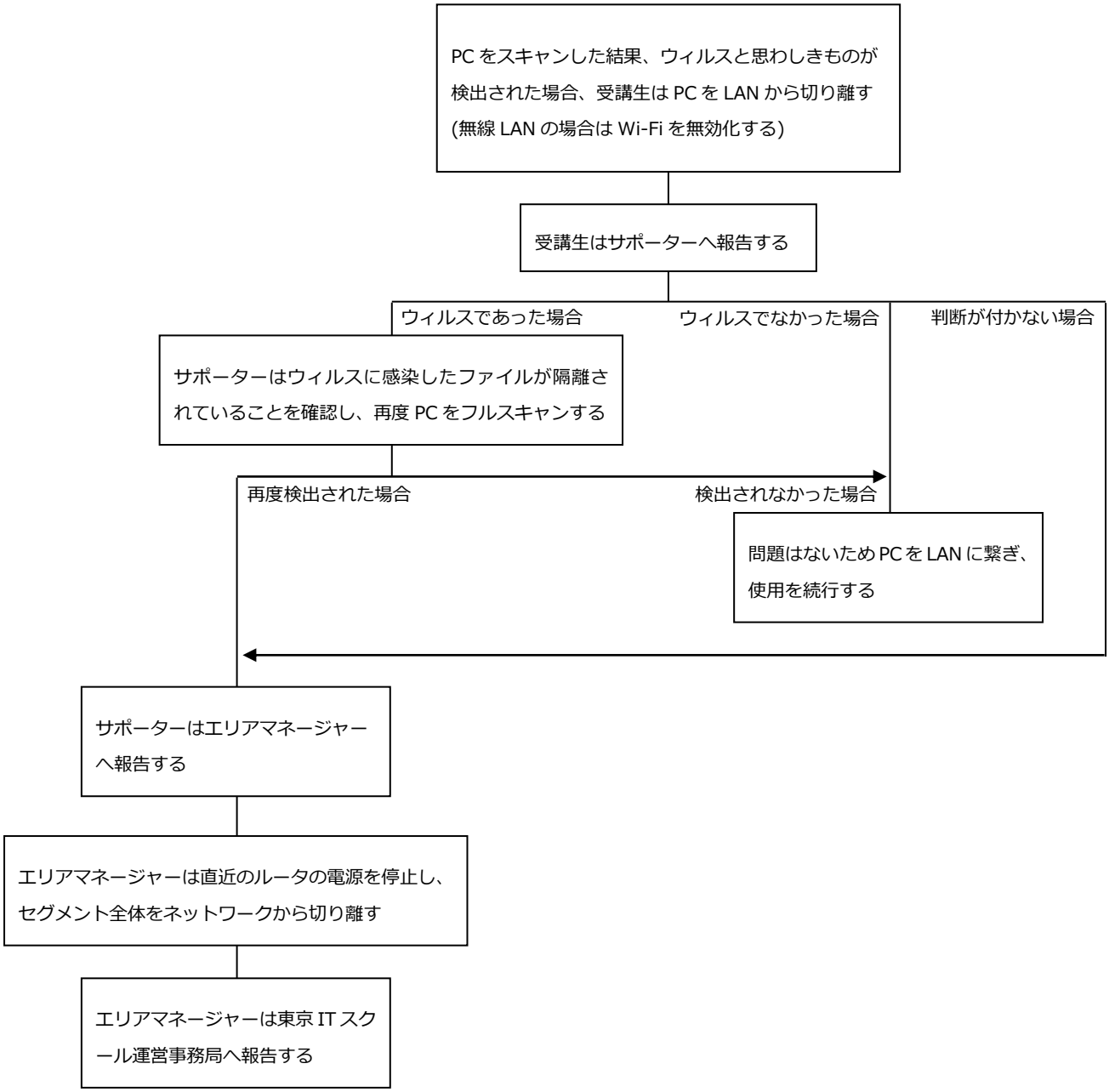
（1）鞄や手荷物は電車の網棚等に置かない。肌身離さず所持する
（2）車中に鞄や手荷物を放置しない
（3）離席・退出時に指差し確認、振返り確認を励行し、置忘れや紛失を防ぐ

7. 作業場所における事故対応と報告について

1　インシデント発生時の対応

インシデントが発生した場合は、原因の追究と対策に努めること。以下にその手順を示す。

（1）作業場所においてウィルスが検出された場合

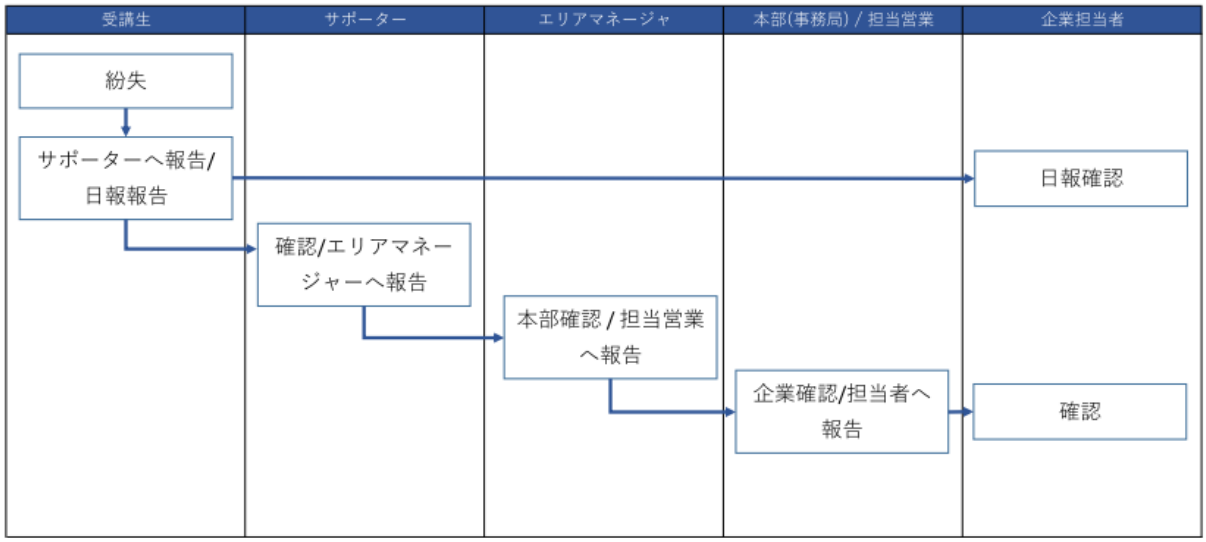


7. 事故対応と報告について

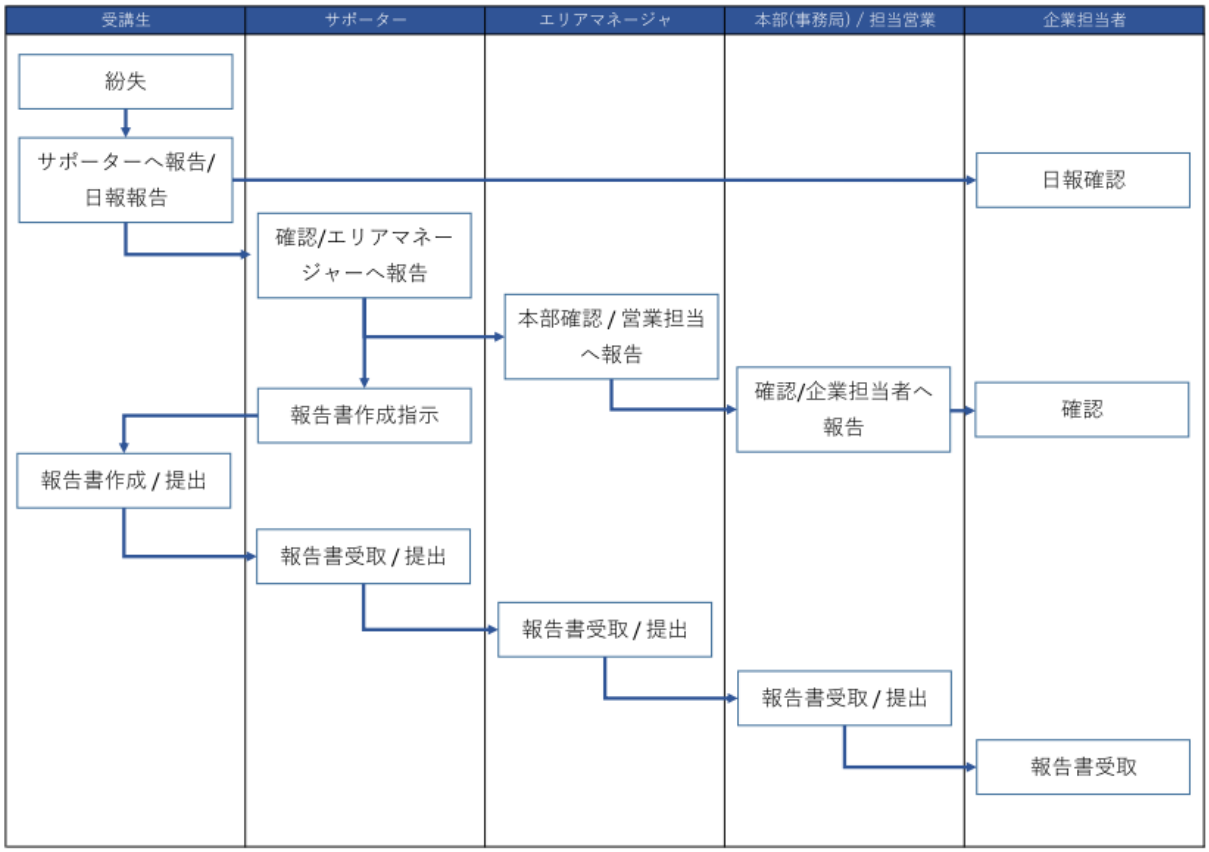
（2）入館証を紛失した場合

受講生が紛失した場合の手順を以下に記す

受講生　1 回目



受講生　2 回目



※入館証を紛失した場合は自宅へは戻らず一時貸出用の入館証を利用する。

2　インシデントの管理

次のインシデントが発生したときまたはその疑いを発見したときは、発見者及び当事者は報告の定めの通り行動を起こさなければならない。

（１）秘密情報等の盗用、悪用、流出、漏洩、紛失、改竄、破壊行為
（２）ワーム、ウィルスによるネットワーク、PC の被害
（３）器物損壊、紛失、盗難、強盗（鍵、セキュリティカード、情報機器等）
（４）情報の破壊や滅失等を伴うソフトウェアの障害
（５）個人の名誉毀損、ネット上でのプライバシーの侵害や誹謗、中傷となる書き込み
（６）不正コピー等の知的所有権の侵害
（７）法令、規程、ルール等の違反

8. その他

1　自社との連絡手段

前述の通り、作業会場内における PC を用いた Web メールのやり取りは禁ずるため、自社との連絡手段は携帯電話、スマートフォンによる電話、Web メールに限る。ただし、講義中に自社から緊急の連絡があった場合は、研修会場外で携帯電話、スマートフォンの操作を行うこと。なお、講義中携帯電話、スマートフォンはマナーモードとすること。

2　自宅における PC の取り扱い

LMS を経由して自宅の PC から研修会場の PC にファイルを送ることは許可されている。
ただし、ファイルのウィルス感染を留意して、ファイルを開く前にウィルススキャンを行うこと。また、自宅の PC のウィルス感染に留意すること。週 1 回のウィルススキャンを接続済みのドライブ全て行うことを推奨する。弊社資産の資料等を LMS 以外のオンラインストレージの利用は不可とする。ブログや SNS への転載及び商用利用の禁止とする。

以上