社外秘（社員、協力会社社員のみ参照および配付可）

情報セキュリティ・個人情報保護
および環境保護
教育テキスト

第 4.0 版
2021 年 03 月 29 日

株式会社 CIJ
人材開発・事業支援室

改 訂 履 歴

版番	改訂日付	改訂項目	承 認	審 査	作 成
1	2017. 12. 04	新規作成	茨木 暢靖	戸田 弘美	藤原 三規男
2	2019. 04. 04	パスワードの定期変更不要、ランサムウェア、契約終了・退職者に対する注意事項、改正個人情報保護法、他	茨木 暢靖	戸田 弘美	藤原 三規男
3	2020. 04. 21	2020 年度の追加事項、他	茨木 暢靖	戸田 弘美	藤原 三規男
4	2021. 03. 29	標的型攻撃の解説等追記、在宅勤務時の私物 PC 取り扱い追記、他	茨木 暢靖	戸田 弘美	小金丸 琢也

目次 ※目次については、前版からの更新箇所を赤字で示していません。

本テキストのねらい

本テキストは、情報セキュリティ・個人情報保護編、環境保護編の二部構成となっています。

(1) **第一部　情報セキュリティ・個人情報保護編**

私たち従業者が、本テキストを読み、セキュリティ事故防止の基本行動を実施することで、セキュリティマインドを醸成し、情報セキュリティ事件・事故の抑止力をつけることをねらいとしています。個人情報保護も含みます。

関連：「『情報セキュリティマニュアル』 7.支援 7.2.力量」

(2) **第二部　環境保護編**

私たち従業者が、会社の環境方針の基本理念および基本方針を理解し、環境に配慮した企業活動を実施することをねらいとしています。

関連：「『環境マニュアル』 7.支援 7.2.力量」

第一部　情報セキュリティ・個人情報保護編

1. 情報セキュリティカード

全従業者に配付している情報セキュリティカードには、情報セキュリティ事故防止の基本行動を徹底するために心掛けるべき、以下のことが記載されています。情報セキュリティカードは常時携行するよう、お願いいたします。なお、印刷用データは社内 HP（「プライバシーマーク／情報セキュリティ」-「情報セキュリティカード」）にも掲載しています。

1.1 社員、協力会社共通

事故防止のため以下のことを常に心掛ける。

(1) お客様の業務情報の無断持ち出しは、絶対にしない。

(2) お客様や会社に関連するものを持っているとき、通勤等の移動時は、常に紛失、盗難に注意を払う。

① カバン等は、電車などでは、網棚/足元に置かず、着席時は「ひざの上」に置く。

② ノート PC や記録媒体に格納した情報は必ず暗号化する。

(3) 入館カードは、決して紛失しないように注意を払う。

① 通勤等の移動時は、カバンの中の頻繁に取り出すものと別の場所に入れる。

② 昼食等で外出する時は、胸ポケットにしまう等、首から吊り下げたままにしない。

(4) 電子メール、FAX は、誤送信防止のため、送信前に必ず相手先が正しいか確認する。

＊ お客様先に常駐するメンバーは、(2)、(3)、(4)に関してお客様のルールと異なる場合、お客様のルールに従うこと。

(3)②に関するお願い：
胸ポケットやカバンにしまう場合は、外出中にしまい損ねる事故を避けるため、必ず外出前にしまうよう、お願いいたします。

1.2 社員

事故発生時には以下の対応を行う。

(1) 当事者は、一人で判断せず、直ちに部門の緊急連絡先に報告し指示を仰ぐとともに、セキュリティ担当に事故状況を報告

(2) 緊急連絡の受付者は、下記の時、お客様への連絡者を通じて直ちに最優先でお客様に第一報を行う。

① お客様から借用した物品を紛失、盗難、破損した場合

② メールや FAX の誤送信、業務情報が書かれた紙の資料の紛失などお客様の業務情報を紛失、盗難、漏洩した場合

(3) 緊急連絡の受付者は、入館カード、携帯電話等は失効の手続きを指示する。メールや FAX の誤送信時は誤送信先への削除依頼と確認を指示する。

(4) 緊急連絡の受付者は、紛失・盗難の場合は警察、交通機関、施設に紛失・盗難の問合せと紛失届・盗難届の提出を指示する。

＊ 自分が当事者になった場合に備えてあらかじめ部門の緊急連絡先とセキュリティ担当の連絡先を確認しておく。

1.3 協力会社

事故発生時には以下の対応を行う。

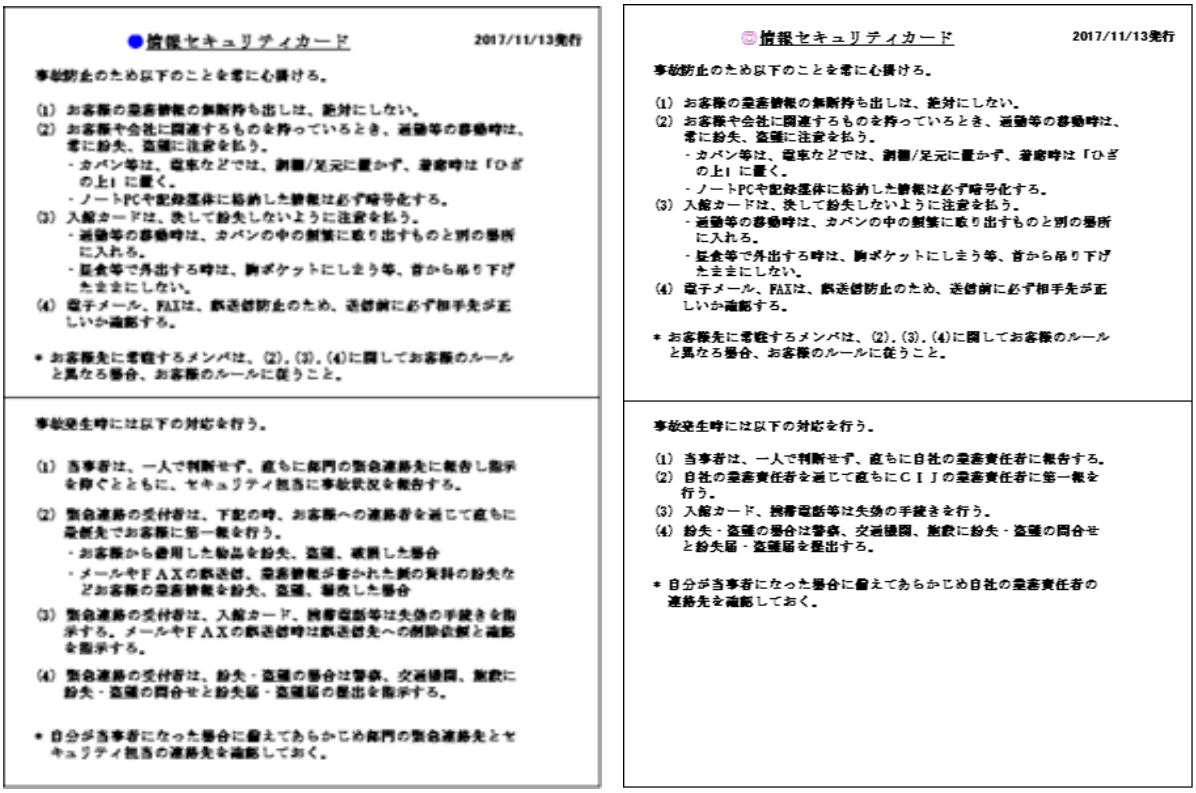
(1) 当事者は、一人で判断せず、直ちに自社の業務責任者に報告する。

(2) 自社の業務責任者を通じて直ちに CIJ の業務責任者に第一報を行う。

(3) 入館カード、携帯電話等は失効の手続きを行う。

(4) 紛失・盗難の場合は警察、交通機関、施設に紛失・盗難の問合せと紛失届・盗難届を提出する。

＊ 自分が当事者になった場合に備えて、あらかじめ自社の業務責任者の連絡先を確認しておく。



●情報セキュリティカード　2017/11/13発行

事故防止のため以下のことを常に心掛ける。

(1) お客様の業務情報の無断持ち出しは、絶対にしない。
(2) お客様や会社に関連するものを持っているとき、通勤等の移動時は、常に紛失、盗難に注意を払う。
・カバン等は、電車などでは、網棚/足元に置かず、着席時は「ひざの上」に置く。
・ノートPCや記録媒体に格納した情報は必ず暗号化する。
(3) 入館カードは、決して紛失しないように注意を払う。
・通勤等の移動時は、カバンの中の個装に取り出すものと別の場所に入れる。
・昼食等で外出する時は、胸ポケットにしまう等、首から吊り下げたままにしない。
(4) 電子メール、FAXは、誤送信防止のため、送信前に必ず相手先が正しいか確認する。

＊ お客様先に常駐するメンバは、(2)、(3)、(4)に関してお客様のルールと異なる場合、お客様のルールに従うこと。

事故発生時には以下の対応を行う。

(1) 当事者は、一人で判断せず、直ちに部門の緊急連絡先に報告し指示を仰ぐとともに、セキュリティ担当に事故状況を報告する。

(2) 緊急連絡の受付者は、下記の時、お客様への連絡者を通じて直ちに電話でお客様に第一報を行う。
・お客様から借用した物品を紛失、盗難、破損した場合
・メールやＦＡＸの誤送信、業務情報が書かれた紙の資料の紛失などお客様の業務情報を紛失、盗難、暴露した場合

(3) 緊急連絡の受付者は、入館カード、携帯電話等は失効の手続きを指示する。メールやＦＡＸの誤送信時は誤送信先への削除依頼と確認を指示する。

(4) 緊急連絡の受付者は、紛失・盗難の場合は警察、交通機関、施設に紛失・盗難の問合せと紛失届・盗難届の提出を指示する。

＊ 自分が当事者になった場合に備えてあらかじめ部門の緊急連絡先とセキュリティ担当の連絡先を確認しておく。

●情報セキュリティカード　2017/11/13発行

事故防止のため以下のことを常に心掛ける。

(1) お客様の業務情報の無断持ち出しは、絶対にしない。
(2) お客様や会社に関連するものを持っているとき、通勤等の移動時は、常に紛失、盗難に注意を払う。
・カバン等は、電車などでは、網棚/足元に置かず、着席時は「ひざの上」に置く。
・ノートPCや記録媒体に格納した情報は必ず暗号化する。
(3) 入館カードは、決して紛失しないように注意を払う。
・通勤等の移動時は、カバンの中の個装に取り出すものと別の場所に入れる。
・昼食等で外出する時は、胸ポケットにしまう等、首から吊り下げたままにしない。
(4) 電子メール、FAXは、誤送信防止のため、送信前に必ず相手先が正しいか確認する。

＊ お客様先に常駐するメンバは、(2)、(3)、(4)に関してお客様のルールと異なる場合、お客様のルールに従うこと。

事故発生時には以下の対応を行う。

(1) 当事者は、一人で判断せず、直ちに自社の業務責任者に報告する。
(2) 自社の業務責任者を通じて直ちにＣＩＪの業務責任者に第一報を行う。
(3) 入館カード、携帯電話等は失効の手続きを行う。
(4) 紛失・盗難の場合は警察、交通機関、施設に紛失・盗難の問合せと紛失届・盗難届を提出する。

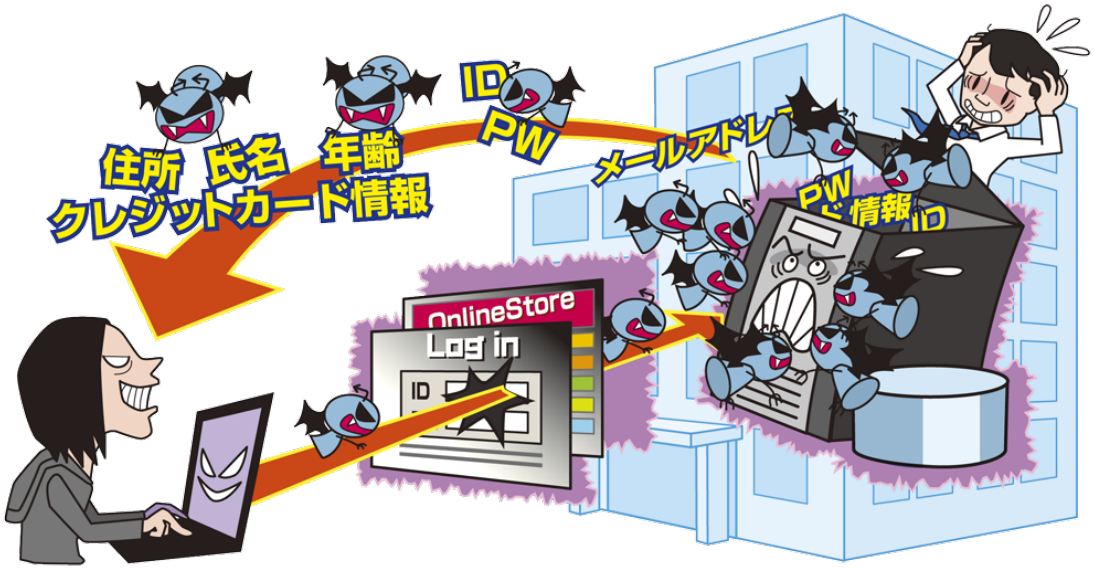
＊ 自分が当事者になった場合に備えてあらかじめ自社の業務責任者の連絡先を確認しておく。

図 1-1　情報セキュリティカード（社員用、協力会社用）

2. 情報セキュリティ事故

2.1 事例

(1) SQL インジェクション対策事件（2014 年 1 月 23 日判決）



情報処理推進機構（IPA）情報セキュリティ 10 大脅威 2018 より
https://www.ipa.go.jp/security/vuln/10threats2018.html

インテリア販売の X 社が運営する EC サイトが外部からの SQL インジェクションによる不正アクセスを受け、最大 7,316 件のクレジットカード情報が漏洩した。

X 社は謝罪や調査等の対応および、売上減少による損害等に関し、システム開発会社の Y 社に対し、委託契約の債務不履行に基づき 1 億円余りの損害賠償を請求、東京地裁に起訴した。

その結果 X 社が勝訴し、東京地裁は Y 社に約 2,262 万円の損害賠償金を支払うよう命じた。判決では、X 社から Y 社に対しセキュリティ対策について指示はなかったが、Y 社は必要なセキュリティ対策を講じる義務があったとのことで、それを怠ったため Y 社の債務不履行となった。

SQL インジェクションとは、アプリケーションが想定しない SQL 文を実行させることにより、DB システムを不正に操作する攻撃方法のことです。

SQL インジェクションに限らず、開発会社側は、例え契約になくても（契約に明記されていることが望ましい）広く一般的なセキュリティ対策 は取る必要があります。

CIJ の人材開発・事業支援室（CBD）では、開発者に最新のセキュリティ関連の事故や脅威を知り、セキュアな Web アプリケーション開発における注意点を理解してもらうため、下記研修を提供しています。ご活用ください。

WebAP 技術教育「Web サイトセキュリティ研修」

（研修で使用しているテキスト「CIJ セキュア開発ガイドライン」は、Leaf で参照可能（CIJ 社員のみ））

(2) 日本年金機構の個人情報流出事件（2015 年 6 月 1 日発表）

情報処理推進機構（IPA）情報セキュリティ 10 大脅威 2018 より
https://www.ipa.go.jp/security/vuln/10threats2018.html

2015 年 5 月 8 日、日本年金機構でマルウェアが組み込まれた電子メールの添付ファイルを少なくとも 2 人の職員が開封し、端末が感染。その結果、基礎年金番号や氏名などを管理するシステムが不正アクセスを受け、情報が流出した。

流出したと考えられる情報は約 125 万件である。そのうち、約 55 万件は内規で定められている暗号化が実施されていなかった。また、マルウェアの通信を検知した 5 月 8 日の段階で通信を遮断していなかった。さらに、6 月 1 日の発表前に 2ch のスレッドに「職員と思われる」本件の書き込みがあった点で、職員のモラルも問題ありとされた。

機構に百数十通送られたという標的型攻撃メールを開いたのは数人だけで、他の職員は攻撃を見抜き、添付ファイルを開かなかった。そのため、攻撃を認知した場合に共有する仕組みがあれば、被害が抑制できていたかもしれない、といわれている。

2.2 情報漏えいの影響

個人情報や機密情報の漏えいにより、以下に示す「損害賠償の請求」、「社会的信用の失墜」、「就業規則に基づく懲戒」のすべてが起こり得ます。個人情報や機密情報のずさんな管理によって社会的な信用を失うことが、事業者にとって最大の損失です。

(1) 損害賠償の請求

個人情報を漏えいした場合、「個人情報保護法」によって罰則が科される可能性がある。

(a) 1 年以下の懲役または 50 万円以下の罰金。また会社にも 1 億円以下の罰金が科せられる。

(b) 損害賠償については、漏えいした情報 1 件当たり 5,000 円～1 万円程度が相場であり、漏えいした内容、人数によっては莫大な損害賠償が必要。

(2) 社会的信用の失墜

会社は個人情報を漏えいした社員の監督責任があり、責任を問われる。

(a) 会社の社会的信用の失墜。

(b) 商談が破談、取引先の喪失。

(c) 被害者からの問合せ対応により、通常業務が回らない。

(3) 就業規則に基づく懲戒

社員は就業規則等（社員就業規則第 33 条（懲戒）の適用に関する規則等）による懲戒の対象になる。

個人情報や機密情報を漏えいしないよう、十分に気を付けてください。万一、個人情報や機密情報が漏えいした場合、または、その可能性がある場合、直ちに上長に報告し、指示を仰いでください。

3. セキュリティ事故防止のための基本行動

情報セキュリティへの認識を高め、維持し、セキュリティ対策を確実に実施しましょう！

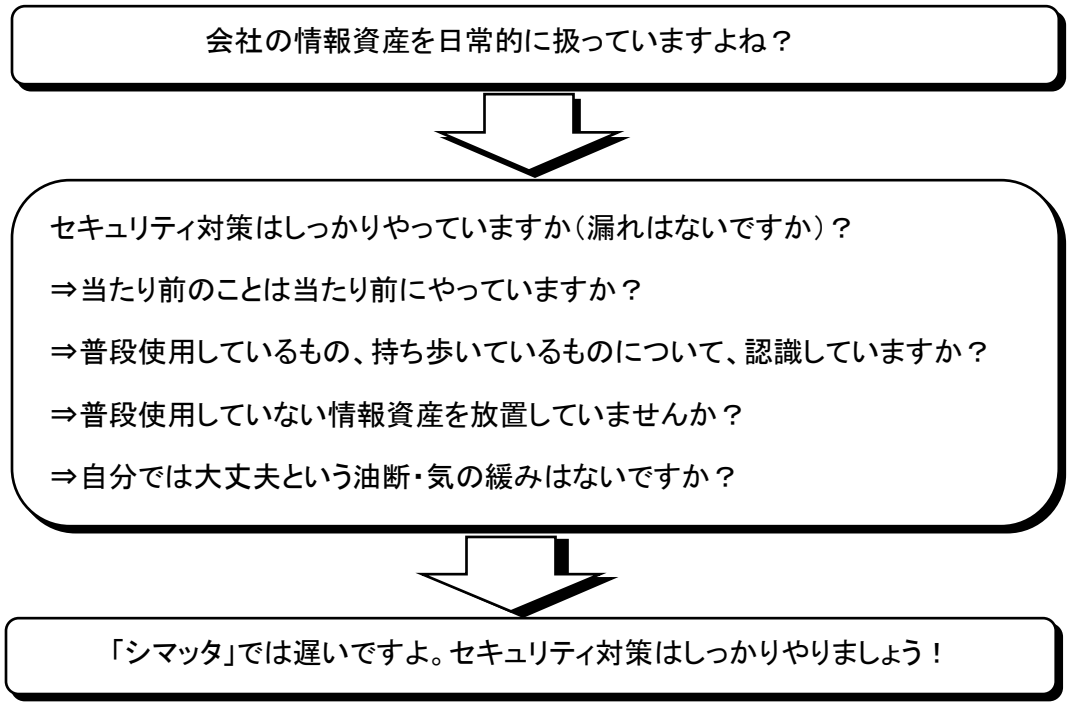


図 3-1 セキュリティ対策の考え方

3.1 業務情報へのアクセス制限

(1) 業務情報※1 を扱う PC、サーバにはユーザ ID、パスワード※2 等によるアクセス制限を掛けること。アクセス権の管理は、部門やプロジェクトの中で責任を持って実施してください。メンバーがプロジェクトの担当を外れた場合、ファイルサーバの管理者は、メンバーが当該プロジェクトの情報にアクセスできないようにしてください。但し、メンバーが以前の担当プロジェクトの保守や瑕疵修補を引続き担当する場合は、除きます。

(2) 業務情報を含む書類・電子媒体は、未使用時には安全に保管すること（重要な業務情報は、鍵を掛けて保管すること）。

※1 業務情報で秘密情報とされるものには、具体的には以下のようなものがあります。

(a) 開発資料全般
  ① 仕様書、ソースリストなどの成果物（中間成果物や古いバージョンのものを含む）
  ② 開発業務で作成した資料（故障処理票、テスト仕様書など開発に関するあらゆる資料）
  ③ 工程管理資料、議事録、報告書など

(b) 業務に係る情報を記述したメモ（書き損じを含む）、印刷ミスした資料

(c) その他
  ① お客様情報、協力会社情報、案件情報などの「営業・購買関連資料」
  ② 契約書、注文書、発注書、見積書などの「契約関連資料」
  ③ 事業計画書、予算書、勤怠、評価、社員情報などの「組織運営関連資料」

なお、業務情報だが秘密情報でないものの例として、書籍、Web などで一般に公開されているものがあります。

※2 パスワード流出の可能性がある等、パスワードの変更が必要な場合は速やかに変更する。
パスワードの定期的な変更は不要とする。

以下を参考に、安全なパスワードに変更してください（定期的な変更は不要です）。

(1) 総務省の推奨事項
https://www.soumu.go.jp/main_sosiki/joho_tsusin/security/basic/privacy/01-2.html
  (a) 名前など個人情報から推測できないこと
  (b) 英単語などをそのまま使わないこと
  (c) アルファベットと数字が混在していること
  (d) 適切な長さの文字列であること
  (e) 類推しやすい並び方や、安易な組み合わせにしないこと

(2) 内閣サイバーセキュリティーセンター（NISC）の推奨事項
https://www.nisc.go.jp/security-site/files/handbook-all.pdf （第 1 章に記載あり）
  (a) ログインパスワードは、少なくとも“英大文字小文字+数字+記号で 10 桁以上”
  (b) より長くして安全性を高めるにこしたことはない
  (c) パスワードの使い回しをしない（似たパスワード、法則性のあるパスワードも不可）

3.2 業務情報の社外への持ち出し禁止

(1) 業務情報を職場から持ち出すことを原則として禁止する。
(2) やむを得ない事情があり業務情報を職場から持ち出す場合には、セキュリティ対策を実施の上、「ノートパソコン等持出・持込申請書／許可書」を申請して管理者の承認を得る。
(3) 業務情報を持ち運ぶ場合は、下記のことを守る。
  (a) 飲酒はしないこと。
  (b) 移動中は、業務情報の入ったカバン等を体から離さないこと。
  (c) 職場基点、合理的なルートでの移動を原則とし、不要な場所には立ち寄らないこと。
  (d) 業務情報をカバン等から取り出した場合は、業務終了後、確実に戻すこと。
  (e) 万一紛失した場合は、直ちに部門の緊急連絡受付者（上長など）に報告し、指示を仰ぐこと（置忘れなどにより一時的に紛失したものの見つかった場合も同様）。

3.3 情報の収集

情報の収集は、業務の遂行上必要であり、業務目的を満たす範囲内でのみ行ってください。業務の目的から外れた情報の収集または、不正な手段や一般倫理から外れた手段による情報の収集は行ってはなりません。例えば、あるお客様のプロジェクトの業務情報を、同じお客様の他のプロジェクトや他社のプロジェクトに流用してはなりません。なお、収集した情報は情報資産台帳で管理し、以下に示す機密性（極秘、秘密、公開）の分類に準じて取扱ってください。

(1)「極秘」とは、厳重なる管理を要する情報であり、最小限の取扱者以外への公開を禁ずるもの
(2)「秘密」とは、管理を要する情報で、社内の関係者以外に公開を禁ずるもの
(3)「公開」とは、ある一定の条件は付くが、社外に公開してもかまわない情報

3.3.1 個人情報の収集

個人情報を収集する場合には、上記に加えて下記の点にも注意してください。

(1) 過去に収集した個人情報とは異なる新しい種類の個人情報を収集する場合は、「新規個人情報取得・廃棄申請書」を使用し、個人情報保護部門管理者と個人情報保護管理責任者の承認を得る。
(2) 個人情報のうち、人種、信条、又は宗教等、「個人情報保護管理規則」（第９条）に定める要配慮個人情報は、原則として、予め本人の同意を得ないで取得してはなりません。
(3) 個人情報を本人から直接書面によって取得する場合は、「取得時の必要通知事項文面」またはそれに相当する文書を事前に提示し、本人の同意を得た上で行う。
(4) 個人情報を直接書面以外の方法によって取得（委託を受けた、提供を受けた、公開情報から取得した等）した場合は、予めその利用目的を公表している場合を除き、速やかに利用目的を本人に通知するか、または公表する。詳細は、「個人情報保護管理規則」（社内

HP「プライバシーマーク／情報セキュリティ」-「個人情報保護関連文書(規則他)」-「規程・規則」)を参照してください。

(5) 特定個人情報(マイナンバーを内容に含む個人情報)を取扱う業務を協力会社に委託する場合、「特定個人情報等保護に関する契約書」、「特定個人情報等保護に関する覚書」の締結と、別途「秘密保持契約書」の締結も必要です。様式については、社内 HP の「法務・監査室」配下にある「契約書標準様式」を参照してください。

3.4 私物による業務情報の取扱い禁止

(1) 私物のノート PC・USB メモリ等の外部記憶媒体を職場に持ち込むことを禁止する。

(2) 私物のノート PC・USB メモリ等の外部記憶媒体を使用し、業務情報を取扱うことを禁止する。
ただし例外として、「AnyClutch Remote」「マジックコネクト」等のシンクライアントソフトの使用を会社より許可された従業者は、当該ソフトを私物 PC にインストールして、業務利用できる。
※ 業務利用 する私物PC は、「PC 管理手順書」の「4. 1 PC の利用 」(1)項から(4)項および(9)項に従う必要があります。詳しくは「PC 管理手順書」を参照してください。
※ 会社 PC 側の業務情報を私物 PC にファイル転送やコピー＆ペーストしたり、内容を書き写したりする行為は情報漏洩に繋がるため禁止です。

(3) 業務情報を取扱うメールの送受信に、私的利用のメールアドレスを使用することを禁止する。私的利用のオンラインストレージサービス、ファイル転送サービス、オンラインアプリケーションサービス、ブログ、フェイスブック、ツイッター等を使用し、業務情報を取扱うことを禁止する。

3.5 Web ページへのアクセスについて

(1) 社外の Web ページへのアクセスは、業務上必要な範囲に限るものとする。会社 PC から私用のメールサービス(Gmail など)にログインするなどの、私的な Web ページアクセスは禁止する。

(2) 業務上必要な範囲において社外の Web ページからファイルのダウンロード等を行う場合には、必ずウイルスチェックを実施すること。

(3) 業務上、会員登録が必要な Web ページへのアクセスが必要な場合は、その都度、所属部門長の許可を得ること。

3.6 秘密文書(秘密データ含む)の取扱いについて

文書は、利用しない時は放置せず、所定の場所に仕舞うようにしてください(クリアデスク)。コピー、FAX した時は、機器上に置き忘れないようにしてください。また、文書は文書が持つ機密性の区分(極秘、秘密、公開の 3 区分)にもとづいて取扱ってください。職場において業務で利用しているすべての文書(業務資料)は基本的に秘密情報として取扱ってください。

特に、文書の保管と廃棄には高いリスクが伴いますので、以下の点に注意してください。

(1) 極秘に区分する文書を保管する場合、紙媒体や CD 等の電子媒体は、鍵の掛る棚・キャビネット等を利用する。また、電子データは、アクセス制限を掛けた部門サーバのフォルダで保管する。

(2) 極秘、秘密に区分する文書を廃棄する場合、紙媒体や CD 等の電子媒体はシュレッダー処理するか、若しくは契約した業者に処分依頼する（各職場の社外秘の取扱いに従ってください）。また、部門サーバ等にある電子データは、速やかに消去する。

3.6.1 管理について

秘密文書の無断持ち出しは絶対にしてはいけません。また、持ち出しの許可を得た場合でも、社外でのコピーおよび第三者の出入りがある場所での閲覧はしないでください。

3.6.2 廃棄について

廃棄した PC、メディアやスマートデバイスから個人情報や機密情報が漏えいすることも少なくありません。作成したファイルや電子メールのデータなどを削除しても、ハードディスクにはデータの痕跡が残っています。これは、ハードディスクをフォーマットした場合も同様です。特殊なソフトウェアを利用することで、削除されたはずのファイルを復元することが可能です。スマートデバイスも同様です。

PC、メディアやスマートデバイスを廃棄する場合には、ライセンス管理の対象となるソフトウェアをすべてアンインストール後、情報漏えい防止対策として以下のいずれかの方法を実施してください。

(1) データ消去用の専用ソフトウェアを利用して、データを完全消去する。

(2) 専門業者のデータ消去サービスを利用して、データを完全消去する。

(3) PC のハードディスクを取り出して、物理的に破壊する。

3.6.3 PC の廃棄について

特に PC を廃棄した時には、下記の社内手続きも忘れずに行ってください。

(1) PC を部門の情報資産台帳から削除するための依頼を部門の情報資産台帳管理者に行う。情報資産台帳からの削除は二重線で上書きする等して、少なくとも 1 年間は残すようにする。

(2) PC を License Guard の管理対象から外すための依頼を SAM 部門管理者に行う。

(3) PC を社内ネットから外すための申請をポストマスターに行う。

以上が終了したところで、事業所で定められた手続きに従い、PC を産業廃棄物取扱い業者に引き渡してください。

3.7 マルウェア対策ソフトウェアの導入

マルウェア感染防止のため以下の対策をお願いいたします。

(1) マルウェア対策ソフトウェアを導入し、常時監視させること。

(2) 定期的（週 1 回以上）に完全スキャン（フルスキャン）実施すること。

なお、在宅勤務で使用する PC（私物 PC または会社貸与 PC）は、下記に従うこと。

① 週始めの在宅勤務開始前に完全スキャン（フルスキャン）を実施し、完了してから業務を開始すること。

② 業務の終了後に簡易スキャン（クイックスキャン）を実施すること。

③ 少なくとも1ヶ月分、スキャン履歴を残すこと（画面キャプチャ、ログファイルなどでエビデンスの提出を求めることがある）。

(3) マルウェア対策ソフトウェアのプログラム、定義ファイルは、常に最新バージョンを使用すること。

3.8 セキュリティパッチの適用

OS、アプリケーションソフトは、セキュリティパッチ（修正モジュール、修正プログラム、アップデートプログラムなどともいいます）を適用し、最新の状態にしてください。

なお、本作業を確実に早く実施してもらうため、CBD より全社員および協力会社員向けに月 1 回（第 2 火曜日の翌日）、「マルウェア感染対策のお願い（〇年〇月）」というメールを発行しています。最低でもこのタイミングで、OS、アプリケーションソフトにセキュリティパッチを適用してください。

3.9 宛先確認の徹底等

メール／FAX の誤送信（添付ミスを含む）や封書の誤郵送により秘密情報が漏えいします。送付先アドレスの確認等には万全の注意を払ってください。

(1) CIJ 事業所内では、CipherCraft/Mail をインストールし、使用すること。

アドレス帳にメールアドレスを登録する場合、以下を実施してください。

(a) 会社別や事業部別にカテゴリー分けする。

(b) フルネーム、会社名などの情報も併せて登録する(同姓同名に注意してください)。

(c) 表示名にフルネーム、会社名などが併せて表示されるようにする。

メールをネットワーク管理者（「owner-」で始まる宛先アドレス）に誤送信するケースが発生していますので、送信先に指定したりアドレス帳に掲載したりしないよう注意してください。誤送信の原因となるため、アドレスの自動補完機能（オートコンプリート）は、必ず「無効」に設定しておきましょう。また、他の事をしながら並行してメール作業したり（ながら作業）、CipherCraft/Mail の送信確認ダイアログで、宛先、添付ファイルなど、それぞれについて無意識に OK 判定したりすることのないようにしてください。

メール等の誤送信のセキュリティ事故は 2020 年度に 7 件、2021 年度上期に 2 件あり、そのほとんどに、**送信前確認を十分にしていなかったこと**が関わっています。特に、次のような思い込みが事故に繋がったケースがありました。
(a) 宛先の表示氏名のみを確認し、正しいメールアドレスを指定できていると思い込んだ。
(b) 添付ファイルの名前のみを確認し、ファイルの中身が正しいと思い込んだ。

このように一部の情報から問題ないと判断しないように、注意してください。

なお、メール本文には重要な業務情報は書かないようにしてください。もしメールでの提供が必要な場合は、暗号化などのセキュリティ対策を実施して添付するなど配慮してください。

(2) 封書の誤郵送がないように、送付先と内容の確認には万全の注意をはらうこと。重要な書類は普通郵便で送らないこと。

(3) FAX の誤送信がないように、FAX 番号の確認には万全の注意をはらうこと。

3.10 不審なメールについて

近年、特定の企業･組織を狙い打ちする「標的型攻撃メール」が多くなっています。実在の企業名や官公庁名をかたり、マルウェアに感染させようとする悪質なメールです。また昨今では、不特定多数に対して攻撃する「ばらまき型メール」や、PCを利用できないようにして復旧するための金銭を要求する「ランサムウェア」も増えてきています。身に覚えのない不審なメールには十分注意してください。

添付ファイルは主に圧縮された実行形式ファイルが用いられ、ファイル名に「.pdf」などの文字を付け加えることで実行形式ファイルであることに気付かれないようになっています。また、ファイルを添付せずメール本文にリンクを記載し、マルウェアファイルをダウンロードさせることもあります。むやみに添付ファイルを開いたり、記載されたURLをクリックしたりしないでください。

メールは運送会社や日本郵政からの配達通知、銀行やカード会社からのお知らせなどを装ったものや、組織や業界固有の用語等を用いたものなど、自然な件名や本文を装っているため注意が必要です。最近の特徴として、送信元のメールアドレスが実在のアドレスを装ったものなど非常に紛らわしくなっていることがあります。

また、実在の官公庁や企業から送られてきたメールであっても、普段から添付ファイル付きのメールをやりとりしている相手でない場合は、送信者に間違いなく送信してきたか問合わせ、送信したとすればどのような添付ファイルかなど確認するようにしてください。

不審なメールに気付いた人は、組織内で情報共有するためにも、CBDに一報を入れるか上長に報告し指示を仰ぐようにしてください。また、未認識の送信元からの受信メールを判別するために、次のようにメールボックスの振り分け設定を実施してください。
(1) 送信元に応じて受信メールを自動的に振り分ける設定をする。
(2) 新しい送信元からの受信メールが増える都度、振り分けの設定を追加する。

（参考1） ランサムウェアについて ※WebやUSBなどを経由して感染することもあります。

コンピュータウィルスの一種であるランサムウェアは、一旦感染すると、データを暗号化したり画面をロックしたりしてPCを利用できないようにした上で、復旧のために身代金（ランサム）の支払いを求めるという非常に悪質なものです。IPA（情報処理推進機構）より発表された「情報セキュリティ10大脅威2020」においても今なおランクインしており、大変危険なマルウェアであるといえます。たとえ身代金を支払ったとしてもデータの復旧が出来ないことも多いため、日頃から以下のような対策をすることが大切です。

(1) 不審なメールやメールの添付ファイルは開かない。また、不審なサイトに行かない。
(2) 不審なメールやサイトに記載された URL はクリックしない。
(3) 不審なソフトウェアはダウンロードやインストールをしない。
(4) セキュリティパッチや更新プログラムを確実に適用する。
(5) 日頃からバックアップを取得する。

（参考2）情報処理推進機構(IPA)のホームページにて、標的型攻撃の手口や対策の解説動画が公開されています。学習教材として、ご活用ください。
https://www.ipa.go.jp/security/keihatsu/videos/

3.11 使用禁止のソフトウェア

社内で使用が禁止されているソフトウェアを以下に示します。詳細は、社内 HP の「情報システム部」-「ソフトウェア資産管理運用情報」-「ソフトウェアリスト」より、「使用禁止のソフトウェア」を参照してください。なお、業務上どうしても使用する必要がある場合は、あらかじめ情報システム部（josys-net@cij.co.jp）と人材開発・事業支援室（pmo@cij.co.jp）に相談してください。

(1) Baidu IME
(2) Evernote
(3) Windows 版の QuickTime
(4) オンラインストレージ（Dropbox、Google ドライブ、OneDrive 等）
(5) ファイル交換ソフト（Winny、Share、BitTorrent 等）

なお、使用許可ソフトウェアについては、社内 HP の「情報システム部」-「ソフトウェア資産管理運用情報」-「ソフトウェアリスト」より、「使用許可ソフトウェア確認ページ」を参照してください。

3.12 クリアスクリーン＆クリアデスク

離席する場合、起動中の PC には以下のいずれかの措置を講じてください（クリアスクリーン）。

(1) パスワード付スクリーンセーバを設定する（5 分を目安とする）。
(2) PC をロックする。
(3) ログオフする。
(4) PC の電源を切る。

また、紙媒体やCDなどの電子媒体は、机の上に放置したまま席を離れないようにし、帰宅時は鍵のかかるキャビネットなどで安全に保管してください（クリアデスク）。

3.13 セキュリティカード（入館カード）管理の徹底

セキュリティカードの取り扱いには十分注意すること。

(1) カバンへの入れ方
頻繁に取り出すものと一緒にすると、取り出し時に落とすことがあるので非常に危険です。セキュリティカードを、ポケット付きの鞄の特定の場所にしまうことを習慣化することが大切です。また、新幹線等車内で席を離れる場合、盗まれないようカバンを持って移動するようにしてください。

(2) 出社時の取出しタイミング
職場までの移動途中ではカバンに仕舞っておき、職場のあるビル内で使用する直前に取り出すようにしてください。

(3) 外出時
セキュリティカードを入れたカバン等は、外出中は手放さない様にしてください（置引きや取違え等に注意）。特に電車などでは、カバン等を網棚／足元に置かず、体から離さないことが大切です。また、飲食時は、セキュリティカードを入れているカバンの存在を意識するようにしてください。

(4) 昼休みなどの外出時
カバンを持たずに外出する時は、職場のあるビル内で、首にかけたまま胸のポケットに仕舞うようにしてください。

(5) 自宅や休日での取扱い
業務外の外出時にはセキュリティカードを持ち歩かないようにしてください。

(6) 点検について
定期的に自主点検し、カードケースの蓋がゆるい、紐が切れそうなど状態が良くない場合は、先延ばしにせずに、すぐに管理者に申し出て交換してください。

なお、お客様先常駐者は、お客様のルールを遵守してください。

入館カードの紛失事故がなくなりません。
カードが入ったカバンの紛失も含め、2020 年度は 7 件、2021 年度上期は 1 件発生しました。

原因として最も多かったものは、以下に例を挙げる **油断の類の思考** でした。
(a) 短時間なら大丈夫だろうと考え、カバンから一時的に離れた。
(b) 財布の中なら大丈夫だろうと考え、入館カードを財布に収納していた。

使用頻度の低い入館カードの場合、セキュリティリスクを考慮した方法（常時所持の回避、定期的な所持確認など）で管理されていなかったことも、その次に多い原因でした。

これらの要因は事故を招く恐れがあるため、行わないよう注意してください。

3.14 定期点検の実施

(1) ひと月又は、ふた月に1回を目安として、セキュリティ定期点検を実施し、記録を残すこと。
(2) 点検項目および実施方法は、部門の実態に合わせて実施のこと。

3.15 スマートデバイスの取扱い

スマートデバイスの取扱いに関して注意事項を示します。詳細は、「スマートデバイス管理手順書」を参照してください。

3.15.1 スマートデバイスの取扱い

(1) スマートデバイスを持って移動しているときは、身体から離さない。
(2) 歩きながらスマートデバイスを使用してはならない、
(3) 電車の中や人が集まるロビー等において、第三者にのぞき見されるような状況でスマートデバイスを使用してはならない。
(4) カメラやビデオで許可のない撮影は行わない(事業所内の作業場所でも同様)。

3.15.2 業務で私物のスマートデバイスを利用する場合の注意事項

(1) 私物スマートデバイスのアドレス帳に、業務で使用する電話番号を登録しても良い。ただし、登録した電話番号は、用途終了(異動、業務終了等)後、速やかに削除すること。
(2) メールの件名、本文、添付ファイルに、漏えいすると問題になる情報(例えば、プロジェクト名、製品名、固有のキーワード等)を記述してはならない。これらの情報を使用する場合は、リスクのない内容(例えば、用語は関係者以外には分からない略語、記号等に置き換える、内容は用件のみ簡潔に示す等)で記述すること。また、私物スマートデバイスを使用しているか否かに関わらず、私物スマートデバイスに向けてメールを発信する従業者も同様に、漏えいすると問題になる情報の取り扱いには留意すること。

(3) スケジュール管理(Googleカレンダー等)は以下の条件を満たす場合のみ利用可能とする。
  (a) スケジュール管理の利用者は特定されており、取扱う情報が利用者以外に公開されることはない。
  (b) 利用者のアクセス権限は明確になっており、利用者に共有されている。
  (c) 漏洩すると問題になる情報は利用者に共有されており、運用時に相互チェックが行われている。
  (d) スケジュール管理の利用は、部長が承認している。

3.15.3 スマートデバイスのセキュリティ対策

(1) 利用するスマートデバイスに対して、パスワード等によるデバイスロックを掛ける。
(2) スマートデバイスの改造（Jailbreak、root 化）をしない。
(3) Android 系のスマートデバイスでは、マルウェア対策ソフトを導入して、常に最新の状態で使用する。
(4) アプリケーションは、信頼できるサイトから購入する。
(5) Android 系のスマートデバイスでは、提供元不明のアプリケーションはインストールしない設定にする。
(6) Android 系のスマートデバイスでは、アプリケーションをインストールする際にアクセス許可を確認する。

3.15.4 その他

私物のスマートデバイスは会社の PC やネットワークとは接続しないでください。充電のみが可能なケーブルに加え、データ転送も可能なケーブルがあり、見分けるのは困難です。そのことも踏まえ、私物のスマートデバイスを PC で充電することも禁止します。

また、会社から貸与されたスマートデバイスを PC に接続する場合も、勝手に接続せず、業務で決められた条件の範囲内で接続するようにしてください。

（補足）2014 年、ベネッセにおいて、派遣社員が顧客の個人情報を名簿業者に売却するという、個人情報流出事件が発覚しました。本件は、スマートデバイスを PC に接続してデータを持出した、とされています。当該派遣社員は逮捕され実刑判決となりましたが、企業もプライバシーマークが取り消され、事件の影響で売上・顧客数が激減し、取締役が引責辞任するなど多大な影響を受けました。

3.16 SNS 利用時の注意事項

SNS（ソーシャル・ネットワーキング・サービス）の取扱いに関して注意事項を示します。詳細は「ソーシャルメディア利用に関する規則」（社内 HP の「総人・経理」-「会社規程」-「その他」。CIJ社員のみ参照可能）を参照してください。

3.16.1 SNS の取扱い

SNSを個人の立場で利用する場合、会社のルールに違反しないよう、その利用に当たっては以下のことに注意してください。

(1) 会社から付与された情報機器（PC、携帯電話、スマートフォン、タブレットなど）を使って、SNSを利用しない。
(2) アカウント登録の際に、業務で使用しているメールアドレスを利用しない。
(3) アカウント名やニックネーム、アイコンなどに、CIJを連想させるものを利用しない。
(4) 勤務先をプロフィールなどに登録しない。

3.16.2 SNS で取扱う情報

SNSで発信・公開する情報については、以下のことに注意してください。

(1) 実生活や公の場で行わない（発信・公開しない）ことは、SNS上でも行わないことが基本である。例えば次のような情報を取扱うことがないように注意する。
  (a) モラルに反した行動や発言、他者を不快にさせるような発言や情報（わいせつな情報、法令違反、差別的発言、他者への誹謗中傷、個人情報など）
  (b) 虚偽や事実と異なる情報、根拠のない情報
  (c) 第三者の著作権・肖像権・商標権など、第三者の知的所有権を侵害するもの
  (d) その他、会社が不適当と指定した情報
(2) 個人の立場でSNSを利用する場合、業務に関連して、例えば次のような情報を取扱わないように注意する。
  (a) 会社の秘密に関する情報（社外秘とされている会社の規則や文章、未公開の自社製品の情報など）
  (b) 会社や社員が関係する事件・事故などに関すること
  (c) 業務上知り得たお客様や取引先をはじめとする関係者の情報（会社名を含む）
  (d) 同僚など社員の個人情報
  (e) 業務内容や仕事上での出来事等

3.17 使用したことのないソフトウェアをインストールする場合の手順

社内 HP の情報システム部配下に「ソフトウェア資産管理運用情報」－「ソフトウェアリスト」があり、以下のように定められています。

(1) 使用許可ソフトウェア確認ページ
ソフトウェアの利用に事前申請が必要かどうか確認することができます。現在使用が許可されているソフトウェアの一覧表示も可能です。

(2) 「ソフトウェアのエンドユース申請書」（提出先は CBD 経由（情シス））
「使用許可ソフトウェア確認ページ」に掲載されていないソフトウェアを使用する場合、事前に「ソフトウェアのエンドユース申請書」を CBD に提出し、許可を得るようにしてください。無償かつ企業での利用が認められている場合でも、「ソフトウェアのエンドユース申請書」の提出は必要です。

また、「ソフトウェア管理規則」第 15 条に従業者の遵守事項が記載されていますので、併せてご確認ください（社内 HP の「総人・経理」–「会社規程」–「開発」）。

3.18 契約終了・退職者に対する注意事項

プロジェクト管理者（または管理者から指名された社員）は、協力会社社員の契約終了または社員の退職時には、「情報セキュリティチェックリスト」を用いて、情報セキュリティ確認を実施してください（チェック済みチェックリストの原紙は、契約終了者または退職者に渡してください。また、部門は台帳を作成し、チェックの記録をお願いします）。

詳細は社内HPより以下をご確認ください。
「協力会社員契約終了・社員退職時の情報セキュリティ確認実施のお願い」
（社内より）http://www.ykhm.cij.co.jp/privacy/notification/20170803.pdf
（社外より）https://www.ykhm.cij.co.jp/privacy/notification/20170803.pdf

「情報セキュリティチェックリスト」は以下の社内HPにあります。
「法務・監査室」－「契約書標準様式」－「２．セキュリティ関連」－「３　情報セキュリティチェックリスト（契約終了者・退職者用）」

なお、チェック項目にも記載していますが、以下の通り、契約終了・退職「後」にも守るべき注意事項がありますので、遵守してください。

(1) 契約終了・退職した後も、秘密情報を開示、漏洩もしくは使用してはならない。
(2) 秘密情報（お客様名、システム名を含む）を履歴書やSNS等に記載してはいけない。
(3) 秘密情報（お客様名、システム名を含む）を面接や新しい職場等で話してはならない。

3.19 個人情報の取扱いについて

個人情報保護法が改正され、社内規約等が改訂されています。個人情報保護法の主な変更点とその概要を表3－1に示しますのでご確認ください。不明な点は、CBD までお問合せください。

表 3-1 改正個人情報保護法の変更概要

#	主な変更点	変更の概要
1	個人情報の追加定義事項	個人識別符号（指紋認識データ等、個人の身体的特徴をコンピュータ利用できる様に変換した符号及び免許証番号等、対象者ごとに異なるように割り振られた文字／記号等の符号）が、新たに個人情報として追加定義された。
2	要配慮個人情報の定義及び取扱の変更	要配慮個人情報（本人の人種、信条、病歴等、その他不当な差別または偏見が生じないようにその取扱いについて特に配慮を要する記述等）を取得する場合、予め本人の同意を得る事。（以前は「機微な個人情報」としていたが、再定義され対象が広がった）
3	個人データ消去努力義務の追加	利用目的との関係で不要となり、定められた保管期間を過ぎた個人データは、予め定められた方法に従って、遅滞なく廃棄または消去する努力義務が規定された。
4	不正使用に関する罰則の追加	不正に個人情報を漏洩させた場合の「個人情報データベース等不正提供罪」が新設された。また不正を働いた従業者だけでなく法人にも両罰規定として罰則が適用される。
5	外国事業者への第三者提供時の規定の追加	グローバル化への対応として、外国の事業者（海外に活動拠点をおいて個人データを取り扱う法人事業者）へ個人データを提供する場合の規定が明記された。
6	匿名加工情報（新規定義）	個人データから特定の個人を識別できず、また復元できない様に加工したものを匿名加工情報として新規に定義し、ビッグデータの利活用を促す。
7	トレーサビリティの確保	情報漏洩時の追跡性を確保する為、第三者との個人データの提供、取得時には、当該第三者及び個人データに関わる事項の確認、記録を取る事となった。
8	オプトアウト規制の強化	オプトアウト（予め本人に対して個人データを第三者提供する事について通知または認識しうる状態にしておき、本人がこれに反対しない限り、同意したものとみなし、第三者提供可能とする）による、個人データの第三者提供時に内閣府外局の個人情報保護委員会への届け出が必要となる等、規制が強化された。

4. 万一、事故を起こしてしまった場合は

セキュリティ事故を起こさないよう気を付けてください。セキュリティ事故を起こした場合、まずは緊急連絡受付者※に報告して指示を仰いでください。特に個人情報に関するセキュリティ事故を起こした場合は、後始末だけでなく、情報サービス産業協会（JISA）へ報告が必要になります（JISA 内部で審議の上、措置事項が示される予定）。個人情報を扱う場合は、個人情報の漏洩や紛失につながらないよう、取扱いに注意してください。

※緊急連絡受付者：セキュリティ事故の当事者の上長などが相当し、部内で定めた緊急事態発生時の連絡先のこと（上長あるいは部門の緊急連絡網の上長につながらなかった場合に備えて、その上位者などの連絡先も確認しておく）。

4.1 セキュリティカード（入館カード）の紛失

セキュリティカードを紛失（特にお客様のセキュリティカードを紛失）した場合は、お客様第一に考え）、速やかに以下の対応を行ってください。

(1) セキュリティ事故の当事者は、一人で判断せず、直ちに発生した事故を緊急連絡受付者に報告し、指示を仰ぐ。併せて、情報セキュリティ担当（事務局／担当役員）にも報告する。紛失後に見つかった場合でも、同様に報告し、指示を仰いでください。

(2) 緊急連絡受付者は、セキュリティ事故の当事者または関係者と協力し、以下の事を実施する。
   (a) お客様のセキュリティカード紛失の場合、お客様にお詫びし、お客様からの指示に従って失効手続きを行う。
   (b) CIJ のセキュリティカード紛失の場合、情報セキュリティ担当の指示に従って失効手続きを行う。

(3) 緊急連絡受付者は、セキュリティ事故の当事者または関係者に対し、紛失物が届く可能性のある公共機関（警察、鉄道会社など）、施設（事業所のテナントビル、立ち寄った飲食店など）に対して、紛失物の問合せと紛失届の提出を指示する。

詳細は、社内 HP の「情報セキュリティに関する緊急事態対応手順」を参照してください。

4.2 スマートデバイス、ノート PC、USB メモリ等の紛失、盗難

スマートデバイス、ノート PC、USB メモリなどを紛失した場合（特にお客様の情報資産を紛失した場合は、お客様第一に考え）、速やかに以下の対応を行ってください。

(1) セキュリティ事故の当事者は、一人で判断せず、直ちに発生した事故を緊急連絡受付者に報告し、指示を仰ぐ。併せて、情報セキュリティ担当（事務局／担当役員）にも報告する。紛失後に見つかった場合でも、同様に報告し、指示を仰いでください。

(2) 被害の重要度を判定し対策を検討するために、緊急連絡受付者は、紛失した情報に関して以下の点について把握する。
   (a) 個人情報、お客様情報、秘密情報が含まれているか。

(b) 情報保護としてはどのような対策を実施していたか（暗号化、ハードディスク保護、認証パスワード保護など）。
(c) 影響はどこにあるか（個人、お客様、自社など）。

(3) 緊急連絡受付者は、セキュリティ事故の当事者または関係者と協力し、以下の事を実施する。
(a) お客様の情報資産であれば、お客様にお詫びし、お客様からの指示に従って遠隔ロック、回線無効化などの手続きを行う。
(b) CIJ の情報資産であれば、緊急連絡受付者の指示により遠隔ロック、回線無効化などの手続きを行う。

(4) 緊急連絡受付者は、セキュリティ事故の当事者または関係者に対し、紛失物が届く可能性のある公共機関（警察、鉄道会社など）、施設（CIJ 事業所のテナントビル、立ち寄った飲食店など）に対して、紛失物の問合せと紛失届の提出を指示する。

詳細は、社内 HP の「情報セキュリティに関する緊急事態対応手順」を参照のこと。

4.3 メールの誤送信

メールを誤送信した場合（特にお客様情報が含まれる場合や他のお客様に誤送信した場合は、お客様第一に考え）、速やかに以下の対応を行ってください。

(1) セキュリティ事故の当事者は、一人で判断せず、直ちに発生した事故を緊急連絡受付者に報告し、指示を仰ぐ。併せて、情報セキュリティ担当（事務局／担当役員）にも報告する。

(2) 緊急連絡受付者は、該当メールおよび添付ファイルの保全をセキュリティ事故の当事者に指示する。被害の重要度を判定し対策を検討するために、緊急連絡受付者は、誤送信したメールに関して以下の点について把握する。
(a) 個人情報、お客様情報、秘密情報が含まれているか。
(b) 情報保護としてはどのような対策を実施していたか（暗号化、パスワード保護など）。
(c) 影響はどこにあるか（個人、お客様、自社など）。

(3) 緊急連絡受付者は、セキュリティ事故の当事者または関係者と協力し、以下の事を実施する。
(a) 誤送信したメールにお客様情報などの重要な情報が含まれる場合、該当するお客様、あるいは本来の送付先にお詫びする。
(b) 誤送信先に対して、お詫びと該当メールの削除を依頼する。またその後、該当メールが削除されたことを確認する。

詳細は、社内 HP の「情報セキュリティに関する緊急事態対応手順」を参照のこと。

4.4 PC のマルウェア感染

PC の利用者は、マルウェアに感染した時、速やかに下記の対策を行ってください。

(1) 使用 PC から LAN ケーブルを外してください。
在宅勤務中の場合は速やかに事業所に連絡し、出社している人に対応を依頼してください。

(2) 無線 LAN、モバイル通信機器を使用している場合には、その機器の特性に従った回線断を行ってください。

(3) 速やかに情報システム管理者（CIJ で作業している場合）に連絡し、その指示に従ってください。

お客様先で作業している場合は、お客様のルールに従って対応してください。

4.5 情報セキュリティに関する重大な違反

情報セキュリティに関する重大な違反を犯した社員に対しては、「就業規則」にもとづいて処分がくだされます。また、協力会社については、契約にもとづいて処置が実施されます。

5. 参考情報

5.1 セキュリティ情報サイト

最新のセキュリティ情報、セキュリティに関する開発者向け情報などを以下の「表 5-1 セキュリティ情報サイト」にまとめました。特に、映像コンテンツは、比較的短い映像が多数提供されており、部内等で参照するのに有用ですので、ご活用ください。

表 5-1 セキュリティ情報サイト

#	項目	URL
1	最新の情報セキュリティに関するニュース（日刊）	https://www.security-next.com/
2	情報処理推進機構（IPA） 情報セキュリティ対策 「情報セキュリティ 10 大脅威 2021」	https://www.ipa.go.jp/security/vuln/10threats2021.html
3	情報処理推進機構（IPA） 情報セキュリティ啓発 映像で知る情報セキュリティ ～映像コンテンツ一覧～	https://www.ipa.go.jp/security/keihatsu/videos/
4	情報処理推進機構（IPA） 資料・報告書・出版物 出版物のご案内 情報セキュリティ白書 2020	https://www.ipa.go.jp/security/publications/hakusyo/2020.html

第二部　環境保護編

1. 環境方針について

CIJ の環境方針を以下に示します。

【環境方針】

(1) 基本理念

株式会社 CIJ は、地球環境の保全が人類共通の重要課題の一つであることを認識し、「クリーン活動」として、企業活動のあらゆる面で 環境に配慮した活動を積極的に推進します。

(2) 基本方針

① 環境マネジメントシステムを確立し、運用し、その有効性を継続的に改善します。

② 事業の推進にあたって、環境に関する法令、規範、及びが同意したその他要求事項を遵守します。

③「クリーン活動」として、下記のことを推進し、環境負荷の低減と汚染予防に努めます。

(a) 紙、電力などの使用量の削減

(b) リサイクルの推進による廃棄物の削減

(c) 業務を通じた環境負荷削減

④ 環境目標を設定し、継続的な改善に努めます。

⑤ この環境方針は、全従業者に周知すると共に、社外に公表し、その達成に努めます。

上記内容は、社内 HP はもとより、社外 HP においても公開しています。環境方針および環境目標に向かって活動することの重要性が記載されていますので、ご確認ください。

2. 環境目標およびその運用について

CIJ では、毎年、環境実施計画書にて、その年度の環境目標を設定し、活動しています。

環境方針に則り、以下の活動を続けています。
(1) 適切なコピー用紙の使用
(2) 適正な電力の使用
(3) ゴミの廃棄等は法令、規範、および CIJ が同意したその他要求事項に準じて実施

2015 年度からは、以下の活動を追加で実施しています。
(4) 環境に良い、CIJ 製品の利用および会議形態の推進
(5) 紙で運用している既存帳票などの電子化推進

(4)は、SONOBA COMET、TV 会議、C-FaCS の活用などにより各部門が実施してください。
(5)は主に管理部門が実施してください。

これらの活動を行うことで環境負荷削減に寄与します。従業者は社内 HP の「環境実施計画書」に目を通し、環境保護に努めるようお願いいたします。

3. 法令順守について

一般ゴミ（燃えるゴミ、缶、瓶、ペットボトル、プラスチック）は各事業所のビル管理会社の規則に従って廃棄してください。PC、プリンタなどの OA 機器、机、書棚などの粗大ゴミ他、通常、就業拠点で一般ゴミとして回収できない廃棄物については、事業所が契約した業者に依頼（本社の場合は、総務人事部に依頼）して廃棄してください。CIJ で決められたルール以外で廃棄すると法令違反となるため注意してください。

CIJ が従うべき法的およびその他要求事項としては、環境基本法や循環型社会形成推進基本法などの他、事業所のある都道府県または市の条例、自社の要求事項があります。 詳細は、社内 HP の「法令・規範」（「順守義務事項一覧」）を参照してください。

―以上―