TCSグループ
関係外秘

情報セキュリティ教育

2025年度　春期版

TCSホールディングス
情報セキュリティ室

ただ今より、TCSグループ『2025年度春の情報セキュリティ教育』を始めます。
この教育では、TCSグループのメンバーとして、知っておくべき重要な事項について確認します。

目次

本教育は、ご覧の順番で進めていきます。

1. 情報セキュリティ教育の目的

第1章 「情報セキュリティ教育の目的」

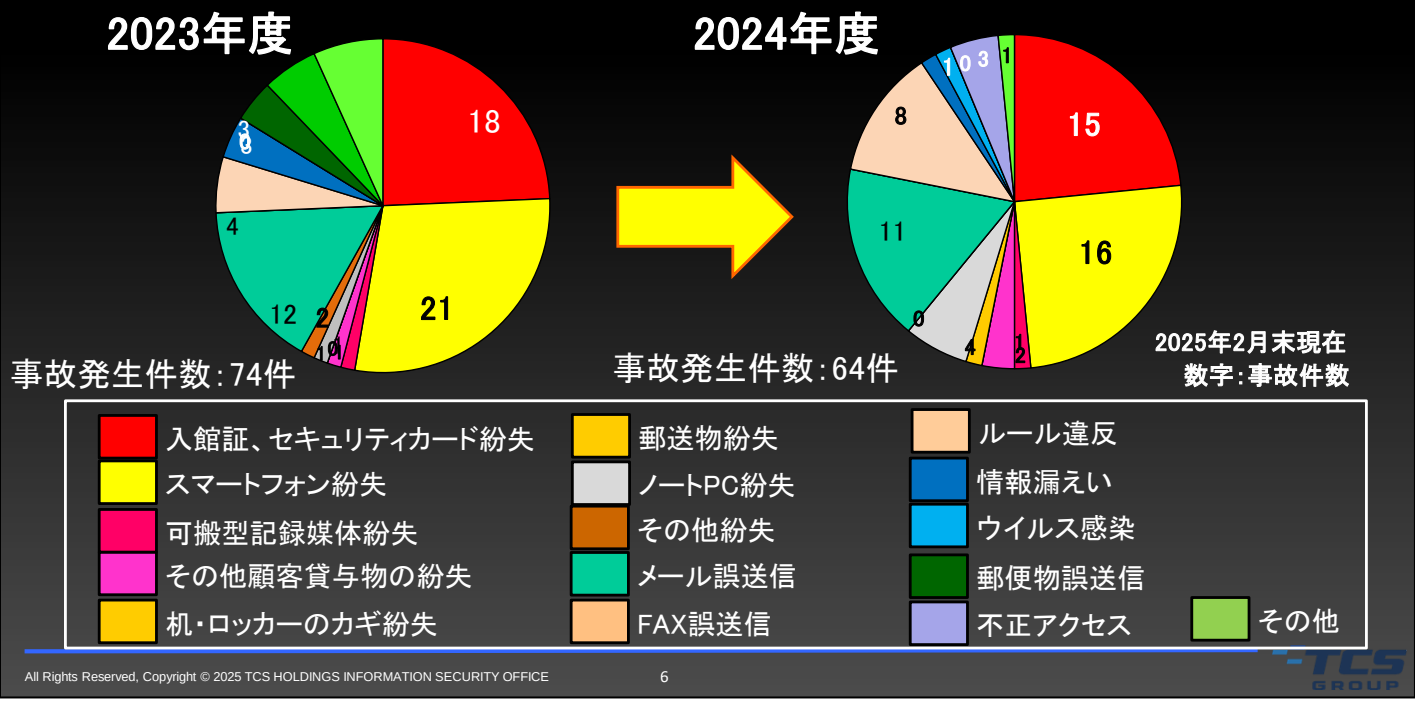
情報セキュリティ教育の目的

この教育の目的は、みなさんが、
「情報セキュリティの必要性と本質を理解」し、
「プロフェッショナルとしての自覚」を持ち、
「TCSグループの業務に携わるメンバーとして情報セキュリティに関して適切な行動」をしていただくことです。
情報セキュリティ事故は、誰にでも起きることと認識し、自らの行動を見直してください。

2. TCSグループの現状

第2章 「TCSグループの現状」

TCSグループ事故発生状況の推移



このグラフはTCS-HD情報セキュリティ室に報告された情報セキュリティ事故をまとめたものです。

2024年度の情報セキュリティ事故は前年度を10件下回る64件発生しました。

紛失系では、スマートフォンや入館証、セキュリティカードの紛失は前年度よりやや減少しました。

また、メールの誤送信は、前年度と変わらず多く発生しています。

この他では、持ち込み規制されているタブレットを客先に持ち込んでしまった、などの顧客ルール違反が増加しています。

情報セキュリティ事故の撲滅に向け、ルールの遵守、対策の実施に努めてください。

情報セキュリティ基本方針

1. 当社グループは、過失、事故、犯罪、災害などの全ての脅威から、
お客様ならびに当社の情報資産を適切に保護します。
2. 当社グループは、情報セキュリティ事故が発生した場合に、
原因究明とその対策を迅速に行い、影響が最小限となるよう努めます。
3. 当社グループは、情報セキュリティ対策に係る規程を定め、
全社員に教育・啓発を行うとともに、遵守の徹底を図ります。
4. 当社グループは、法令ならびにお客様との契約に謳われている
情報セキュリティに関する義務遂行の徹底を図ります。
5. 当社グループは、以上の活動を継続的に改善・実施するための
管理体制を確立し、維持していきます。

※「情報セキュリティ基本方針」より

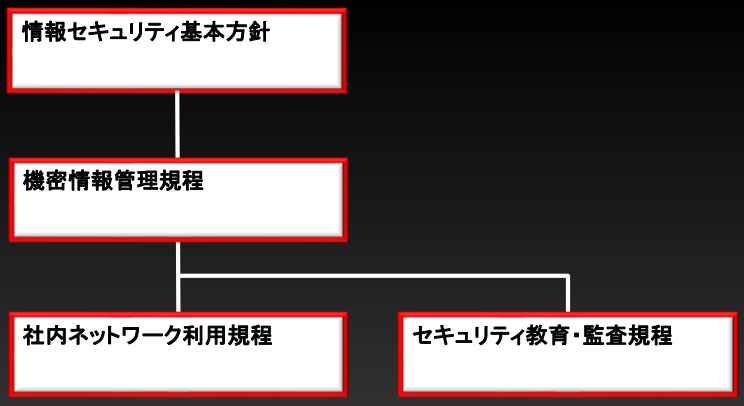
TCSグループは、情報セキュリティ基本方針を社内、社外に対し表明しています。

1. 当社グループは、過失、事故、犯罪、災害などの全ての脅威から、お客様ならびに当社の情報資産を適切に保護します。
2. 当社グループは、情報セキュリティ事故が発生した場合に、原因究明とその対策を迅速に行い、影響が最小限となるよう努めます。
3. 当社グループは、情報セキュリティ対策に係る規程を定め、全社員に教育・啓発を行うとともに、遵守の徹底を図ります。
4. 当社グループは、法令ならびにお客様との契約に謳われている情報セキュリティに関する義務遂行の徹底を図ります。
5. 当社グループは、以上の活動を継続的に改善・実施するための管理体制を確立し、維持していきます。

この方針は私たち全員の宣言でもあります。

2. TCSグループの現状

情報セキュリティ規程とガイドライン構成

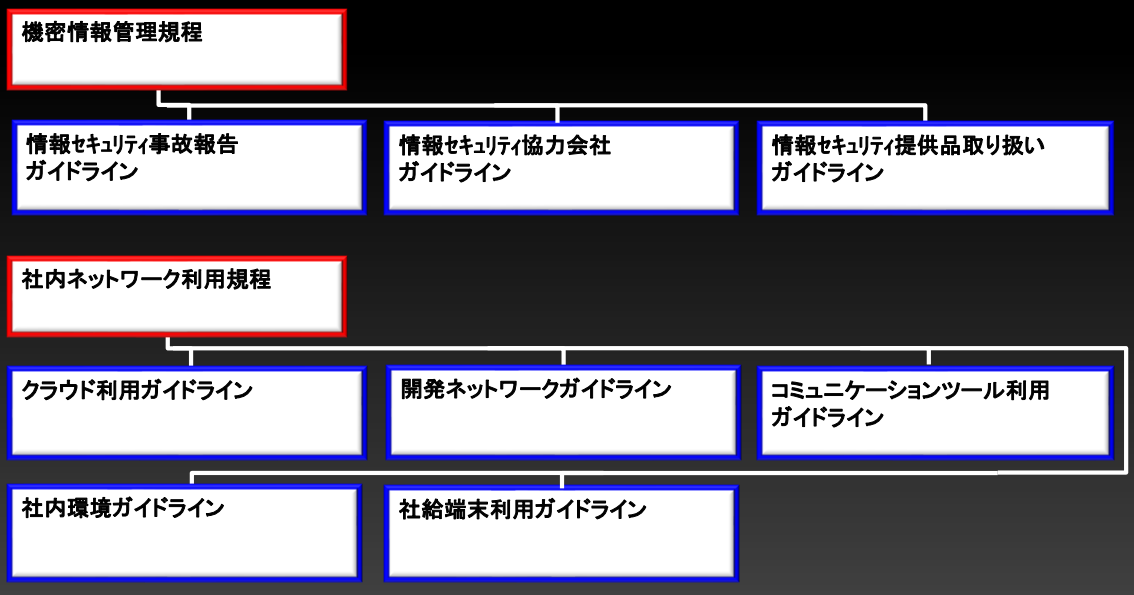


この図は、情報セキュリティ規程の全体構成を示したものです。

全ての規程類は「情報セキュリティ基本方針」を基に構成されています。その中で、「機密情報管理規程」、「社内ネットワーク利用規程」が中心となります。

2. TCSグループの現状

情報セキュリティ規程とガイドライン構成



規程には、具体的に指針を記したガイドラインがあり、
「機密情報管理規程」と「社内ネットワーク利用規程」の配下に設けられています。

なお、2024年度での規定及びガイドラインの変更はございませんが、マーブル統合に伴い、組織名称が「TCS-HD情報セキュリティ委員会」から「TCS-HD情報セキュリティ室」へ変更となりました。

2. TCSグループの現状

情報セキュリティ規程の概要

規程名	内容
機密情報管理規程	「情報セキュリティ基本方針」の遵守すべき事項を網羅的に定めた規程
社内ネットワーク利用規程	社内ネットワーク及び情報システムならびに機密情報を各種脅威から適切に保護するための管理事項を定めた規程
セキュリティ教育・監査規程	会社が取扱う情報の適正管理を実践するために、情報セキュリティに関する教育及び監査事項を定めた規程
個人情報適正管理規程	「労働者派遣法」に基づき、会社が保有または取得するする労働派遣従事者の個人情報の漏えい、紛失、改ざん、誤記録等を防止するための管理を定めた規程
個人情報保護管理規程	「個人情報保護法」に基づき、会社が保有または取得する個人情報の漏えい、紛失、改ざん、誤記録等を防止するための管理を定めた規程
特定個人情報取扱規程	「マイナンバー法」に基づき、マイナンバーに特化した個人情報に対する機密保持、保管管理に関する事項を定めた規程

※情報セキュリティ規程・ガイドラインは各社の「文書管理」に掲示

主な規程の内容を画面に表示します。
これらの規程・ガイドラインは、各社に保管・管理されています。
各自で規程・ガイドラインの確認をしてください。

なお個人情報関連の規程を情報セキュリティ規程として扱っていましたが、マーブル発足を機に情報セキュリティ規程の構成を見直し、人事部に主幹が移動されました。
この教材では、個人情報の扱いの概要について説明します。

3. 情報セキュリティ事故の防止

第3章 「情報セキュリティ事故の防止」

情報資産紛失事故について

- **顧客から貸与されている情報資産を紛失（漏えい）したら**
  - 業務の停止
  - 金銭的な損失
  - 信用の失墜

  などの重大な損失をもたらします。

- **機密情報をテストデータとして使用することは禁止！**

  取り扱うデータが機密情報にあたらないか確認。

私たちは、顧客や会社より情報資産をお借りして業務を行います。
情報資産の中には、顧客情報や社内情報など、機密性の高い情報が含まれている場合があります。
そうした情報資産を紛失してしまった場合、どのようなことが起こるか考えたことはありますか？
情報資産を紛失した場合に起こりえる事象は、大きく分けて以下の3つに分けられます。

業務の停止
情報資産の中には、業務に必要なデータやソフトウェアが含まれている場合があります。これらの情報を紛失した場合、業務に支障をきたし、最悪の場合、業務の停止につながる可能性があります。

金銭的な損失
情報資産の中には、営業秘密や知的財産などの価値の高い情報が含まれている場合があります。これらの情報を紛失した場合、金銭的な損失が発生する可能性があります。

信用の失墜
情報資産の紛失・漏えいなどを起こしてしまった場合、顧客からの企業イメージが著しく低下し社会的信用を失う可能性があります。

直近の事故で、顧客の機密情報をテストデータとして、セキュリティーが定かではない、クラウドサービスにアップロードする情報漏えい事故が発生しています。
機密情報をテストデータとして使用することは禁止です。
業務を行う際は、上記の事象を踏まえて、取り扱うデータが「機密情報」にあたらないかをしっかり確認してください。

情報資産の紛失は、企業や個人にとって重大な被害をもたらします。
そのため、情報資産の管理には十分に注意する必要があります。

また、業務タスクをPJリーダと共有するため、PJリーダや顧客に確認をせずに、
業務タスクを外部サイトに書き出すセキュリティ事故も発生しています。

セキュリティ規程やガイドラインによってルールが定められているように、顧客にもルールが定められています。
そのルールの目的を理解せず、個人の判断で行動しないでください。
定期的に顧客ルールの確認を行い、ルールの順守に努めてください。

3. 情報セキュリティ事故の防止

紛失の原因

- あなたの入館証は大丈夫ですか？

フォルダー
破損

落下や
置き忘れ

網棚や足元に
置かない

定期的に注意喚起をしていますが、入館証の紛失が絶えません。

紛失の原因として、
　カードフォルダーが破損していて、知らぬ間にカードが抜け落ちていた。
　カバンの中に入れていたが、他のものを取り出したとき一緒に出てしまった。
　カバンを電車の網棚に置き忘れた。
　常日頃から貸与物の所在確認をしていなかった。
などが挙げられます。

3. 情報セキュリティ事故の防止

貸与品の紛失予防事例

入館証紛失の予防策

- カードフォルダーやストラップが破損していないか定期的にチェック
  入館証の存在もしっかり確認する
- 入館証は分別収納で紛失リスク低減
- 入館証が入ったカバンは肌身離さず持つ
- 貸与品は移動の度に所在確認し、紛失していないことを確認する
- 在宅勤務時も定期的に所在を確認する

入館証の紛失予防策として
カードフォルダーやストラップが破損していないか定期的にチェックする。
フォルダーだけをチェックするのではなく、入館証の存在もしっかり確認する。

カバンは、入館証だけを入れるためのポケットがあるもの・個別収納ができるものを選ぶなどの工夫をしてください。
入館証が入ったカバンを持ち歩く際は、電車の網棚や足元に置かず、肌身離さず持つようにしてください。
休日にビジネス用カバンを持ち歩いて紛失しないよう、ビジネス用とプライベート用は分けてください。
財布などに入館証を入れ不用意に持ち歩かない等、紛失リスクは最小限になるよう工夫してください。
入館証がフォルダーから抜け落ちる対策として、フォルダーが破損しやすそうな箇所をテープで補強する、またフォルダーがストラップから外れないようにダブルロックするなどの対策を講じてください。

朝、家を出る時・職場から帰る時・家に着いた時に入館証の所在を確認するなど、頻度を増やし確認を習慣化することで早く紛失に気付くことができます。
在宅勤務が続き入館証を使う機会が無くても、定期的に所在を確認してください。
また家族の方が誤って廃棄するケースもあり得ます。保管場所を決めて家族に話しておく、家族からは見つかりづらいところにしまう、など工夫してください。

これらの対策の中には、入館証以外の貸与品管理に当てはまるものもあります。

顧客から情報資産を受け取るときには、いつ、誰から受け取ったのか、必ず記録を台帳などに残し、返却時には返却した情報や物品の内容確認を行ってください。
受け取ったものは定期的に所在を確認してください。
貸与品が不要になった時に返却せず、また返却した時の台帳管理が不十分なことで、事故が発生しています。
管理者は都度適切な対応を行ってください。

情報資産は預かる期間が短ければ短いほど、紛失のリスクは減ります。
使う必要がなくなった情報や入館証などは、速やかに返却してください。

上記ポイントで万全の注意を払い紛失を予防してください。

3. 情報セキュリティ事故の防止

公共の場所での行動

- 業務に関する話をしない
- 書類やPCを広げない

➢ 公共の場所とは…

✓ 一般的:
交通機関、待合室、飲食店、トイレ … など

✓ お客様施設内:
喫煙所、休憩室、トイレ、給湯室、
エレベータホール、セミナールーム、
受付付近 … など

駅のホームで仕事の話をしているのを聞いたことはありませんか？
電車の中で書類を読んでいたり、PCを広げていたりしていることを目にしたことはありませんか？
他人に情報が見えてしまう、聞こえてしまうとそれは情報漏えいです。そのようなことをしてはいけません。

公園や駅など一般の人が共同で利用する公共の場所で業務に関する話を避けるのはもちろんのこと、
顧客先であっても、エレベータ、喫煙所、休憩室、トイレなどの共有スペースは色々な方が出入りします。
一言、二言の会話でも情報が漏えいしてしまうということを認識してください。

飲酒により発生する情報セキュリティ事故

- **飲酒により発生するセキュリティ事故**
  - 置き忘れ（記憶力・注意力が低下）
  - 盗難（酔っぱらいは恰好の的）
  - 破損（足下がふらつき転倒）

- **出張時の飲酒は特に気を引き締めること！**

飲酒をするなら持たない
持っているなら飲酒しない

感染症予防による自粛が解除され、飲酒の機会が増えています。

お酒を飲むと注意力が低下して、
ついうっかりお店や電車内などに入館証の入ったカバンを置き忘れたり、
酔っ払いを狙った窃盗に遭い、貴重品やカバンを奪われたり、足下がふらつき転倒し、
大事なデータが入ったPCや記録媒体を破損させるなど、情報流出や事故につながる場合があります。

このような事故を防ぐために、飲食店などから帰るときは、
・忘れ物が無いか必ず確認する。
・帰りの電車内では、荷物を網棚や足元に置かず、カバンはタスキ掛けする。
など、普段より慎重な行動をして下さい。
ちょっとだけだから大丈夫、お酒は強い方だから大丈夫、
と軽い気持ちで飲み会に参加すると、これらの事故・事件を起こします。
出張帰りの電車内でついリラックスして泥酔し、PCを紛失してしまった事例があります。
PCや重要書類を持って飲酒をしてはいけません。
飲酒する際には、原則として情報資産を持たないようにしてください。

また、記憶が曖昧になるほど泥酔し、カバンや貸与物を紛失する事故も散見されます。
飲酒時には過度の飲酒を控え、飲みすぎている方がいたら注意をしてください。

画面は自動で切り替わります

残り [redacted]

設問1

顧客ルールについて、適切なものを選択しなさい。

1. 顧客先で勤務しているが自社のセキュリティ規程やガイドラインを遵守しているので問題ない。
2. 業務効率化の為、先輩から教えてもらったツールを顧客から貸与されたPCにインストールした。
3. 顧客ルールが変更されていないか、定期的に確認をしている。

TCS GROUP

設問1　顧客ルールについて、適切なものを選択しなさい。
1. 顧客先で勤務しているが自社のセキュリティ規程やガイドラインを遵守しているので問題ない。
2. 業務効率化の為、先輩から教えてもらったツールを顧客から貸与されたPCにインストールした。
3. 顧客ルールが変更されていないか、定期的に確認をしている。

画面は自動で切り替わります

残り [redacted]

設問2

飲酒に関する注意事項について、不適切なものを選択しなさい。

1. 居酒屋で社給スマホを取り出し、来ていたチャットに返信した。
2. 業務後飲み会の予定があったので、PCを持ち帰らず、鍵付きキャビネットにしまってから退勤した。
3. 居酒屋から退店する際に、飲み会参加者同士で忘れ物がないかチェックをした。

TCS GROUP

設問2　飲酒に関する注意事項について、不適切なものを選択しなさい。

1. 居酒屋で社給スマホを取り出し、来ていたチャットに返信した。
2. 業務後飲み会の予定があったので、PCを持ち帰らず、鍵付きキャビネットにしまってから退勤した。
3. 居酒屋から退店する際に、飲み会参加者同士で忘れ物がないかチェックをした。

4. 情報機器の取り扱い

第4章 「情報機器の取り扱い」

社給デバイス

- **社給デバイスを取り巻くリスク**
  - ウイルス感染によるデータ利用不可、PC不正動作
  - 不正アクセスよるアカウント情報の窃盗
  - 紛失・盗難
  - 廃棄時における残留データの漏えい

- **対策**
  - OSやアプリケーションソフトの更新、ウイルス対策ソフトのパターンファイルを更新する
  - 定期的なウイルス検索を行う
  - パスワードを初期値からポリシーに沿ったものに変更する
  - 画面ロック機能を設定する

この章では、主に社給デバイスの取り扱いについて説明します。
社給デバイスとは、会社が貸与した、業務で使用するPC、タブレット、スマホなどのことです。
社給デバイスを取り巻く環境には様々なリスクがあります
・ランサムウェアに感染しデータの利用ができなくなったり、デバイスが正常に動作しなくなる物理的被害
・デバイスへの不正アクセスによるアカウント情報の漏えい
・デバイスの紛失・盗難
・廃棄時における残留データの漏えい
等が挙げられます。

これらリスクへの対策として
　OSやアプリケーションソフトの更新や、ウイルス対策ソフトのパターンファイルを更新する。
　定期的なウイルス検索を行うよう設定する。
　パスワードの初期値をそのまま利用せず、パスワードポリシーに従ったパスワードを設定する。
　画面ロック機能を設定する。
　廃棄時にはデータ消去専用ソフトウェアを使用して、データを復元不可能な状態にする。
といったことが挙げられます。情報セキュリティリスクの対策には完璧はありませんが、1つ1つを確実に実行してください。

社給デバイス

- **業務環境の変化**
  - スマホ活用範囲が拡大している
  - 勤務場所に囚われずに社外から社内リソースへアクセス可能となっている
  - ビデオ会議が増え、ペーパーレス化が一層進展している

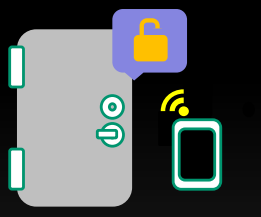
- 社給デバイスの持ち出し機会が増加しているため、持ち出しルールを遵守し、紛失・盗難を防止することが必要

また、TCSグループでは以下のように業務環境が変わってきています。

モバイルPCを持ち勤務場所に囚われずに、社外から社内リソースへアクセスすることも容易になってきました。
さらに会議の様式もビデオ会議が増え、ペーパーレス化が進んでいます。
以上のような変化により、PCを持ち歩く機会が増えたため、PC等の社給デバイスを持ち出す際は、
持ち出しに関するルールを守り、紛失や盗難に遭わないよう一層注意する必要があります。

社給スマホの利用拡大

- **紛失すると･･･**
  - 社給スマホ内、社給スマホアクセス先の機密情報や個人情報を盗まれる
  - 悪意を持った拾得者に執務室へ不正入室される
  - 社員認証ができず業務そのものができない
- **紛失対策**
  - ストラップ等を利用して落下防止する
  - 端末ロックパスワードを設定する
  - 電話帳の内容は必要最低限にする
  - 不要な登録情報は速やかに削除する
  - 遠隔ロックや利用停止等の連絡先を控える
  - 位置情報機能はONにする(推奨）



社給スマホはこれまで電話･メールが主な利用方法でしたが、スマートキー、文書閲覧、ビデオ会議、社員認証など、その利用範囲が拡大してきました。
これに伴い社給スマホが業務に与える影響度も増しスマホ紛失時のリスクがますます高まっています。

社給スマホの紛失事故は後を絶たず、社給スマホを紛失すれば
　社給スマホに格納された機密情報や個人情報を盗まれるだけでなく、社給スマホからアクセスできる情報をも盗まれる可能性がある。
　悪意を持った拾得者に執務室へ不正入室される。
　社員認証ができず業務そのものができなくなる。
などが想定されます。

そこで社給スマホの紛失防止として、あるいは万が一紛失した時に備え、次のような対策を取り事故のリスクを下げる必要があります。
ストラップ等を利用して落下紛失を防止する。
端末ロックパスワードを必ず設定する。
電話帳に登録する電話番号やメールアドレスは必要最低限にする。
登録する氏名や社名は略称にするなど直接特定されないようにする。
不要になった登録情報は速やかに削除する。
紛失･盗難時に速やかに遠隔ロックや利用停止等の対応をとれるよう連絡先を控えておく。
なお、紛失･盗難時に発見できる可能性を高めるため位置情報機能はオン状態にすることを推奨します。

個人所有機器の業務利用

- **個人所有機器の業務利用は禁止**
  - 個人所有機器の感染対策不明のため、セキュリティを保証できない
  - ウイルス感染している可能性から、業務利用で社内感染の恐れ

未許可の個人所有機器

- **顧客先での機器利用の注意点**
  - 顧客が貸し出した機器以外は、未許可の機器
  - 未許可の機器利用を禁止・制限
  - 顧客ルールを理解し、未許可の機器を利用の際は顧客の許可を得る必要がある

TCSグループでは、個人所有の機器（記憶媒体を含む）を許可なく業務に使用することを禁止しています。

これは、個人所有機器のウイルス感染対策が不明であり、セキュリティが保証できないため、業務に利用することで社内感染のリスクがあるからです。

また、携帯性に富んだ記憶媒体は紛失しやすく、機密情報の漏えいの恐れもあります。

さらに、自社貸与機器であっても、顧客先では顧客貸出し機器以外は許可されていないことが多いです。

顧客先のルールを理解し、必ず顧客の許可を得て利用する必要があります。

許可されていない機器を使用するリスクを考慮し、多くの企業がその利用を禁止または制限しています。

なお、TCSグループでは、情報セキュリティ対策として、2025年3月より、使用するUSBについて、システム的に機能制限しており、会社が許可しているUSBでないと読み取りや書き込みが出来ないようになっています。

在宅勤務での注意点

- **利用デバイスの注意点**
  - 社給デバイスで業務を行う。個人所有デバイスは使用禁止
  - 運搬時の置き忘れや盗難に備え肌身離さず
  - 利用しないときは画面ロックをする
  - お子さんのいたずら、家族による無断利用を防止

- **ネットワークの注意点**
  - 原則、在宅勤務時は社給スマホによるテザリング
  - 社給モバイルルータがある場合は、これを使用する
  - 自宅Wi-Fiを利用する場合は直接接続せず、社給スマホによるテザリングで接続する
  - 会社PCと在宅勤務PCの両方にSkyseaを導入する

在宅勤務での勤務は、情報セキュリティ確保のレベルがオフィスよりも劣る環境からインターネットを経由して勤務先のシステム等にアクセスしています。

そのままの状態では情報セキュリティリスクが高い環境であるため、対策を怠ると使用しているPCがウイルスに感染し業務ができなくなる、あるいは第三者により通信を盗み見されることで機密情報が漏えいすることが想定されます。

在宅勤務の時には、以下の注意事項を遵守してください。

社給デバイスで業務を行う。原則、個人所有デバイスを使用することは禁止しています。

社給デバイスの運搬時には、タスキ掛けが出来るカバンやリュックを利用する、網棚に乗せずに膝の上に置くなど、置き忘れ、盗難に備え、肌身離さず持ち運んでください。

社給PCを使わない時や、離席するときは画面ロックをしてください。

小さいお子様によるいたずら、家族による無断使用などの防止のため、できる限り小さいお子様や家族の手が届かない場所で保管してください。

また利用するネットワークについても以下のルールを守ってください。

原則、在宅勤務時は社給スマホによるテザリングでネットワークと接続する。

社給モバイルルータがある場合は、このモバイルルータを使用する。

自宅Wi-Fiを利用する場合も直接接続せず、必ず社給スマホによるテザリングでネットワークと接続する。

社給スマホを挟むことで、外部からの不正アクセスに対して社給スマホがファイアウォールとなり、社給PCを保護します。

TCSグループのVPN接続ではフルトンネリングされていないため、TCS-NETのWebフィルタリングが適用されず、セキュリティが低下します。

VPN利用にかかわらず、在宅勤務時はTCS-NETよりもセキュリティが低下しますので、業務に関係のないサイトの閲覧を避けるなど、Web利用には十分注意してください。

また社給デバイスは、情報セキュリティ事故が発生した場合、アクセス履歴などを確認し事故原因を分析する必要があります。そのため、利用者はPC管理ソフト(SKYSEA)を会社設置PCだけでなく、在宅勤務で利用するPCにも導入しておくようにしてください。

なお顧客から貸与されたデバイスで在宅勤務を実施する場合は、顧客ルールに従って業務を実施してください。

コンピュータウイルス対策

- ウイルス対策ソフトを最新の状態を保ち、
  OS/アプリケーションのアップデートを定期的に行い
  セキュリティパッチを適用すること

- ウイルス感染リスクを意識し、注意を払う
  - ➢ 万が一のためにデータバックアップをしておく

ウイルス対策ソフトを常に最新の状態に保ちましょう。
OSやアプリケーションのアップデートを定期的に行い、セキュリティパッチを適用することで、脆弱性を修正し、ウイルス感染のリスクを減らしましょう。
重要なデータは定期的にバックアップを取り、万が一のウイルス感染やデータ損失に備えましょう。
普段からウイルス感染のリスクを意識し、注意を怠らないようにしてください。

4. 情報機器の取り扱い

コンピュータウイルス対策

- ウイルス感染の疑いを持ったら

対応手順	
感染発覚直後	ネットワークから切断する
	周囲の人へ伝え、感染の拡散を確認
発覚直後の対応後	自社の情報セキュリティ委員へ感染状況を報告し、指示を仰ぐ
委員報告後	手動によるウイルス検索

- ウイルス検知できない場合はウイルス対策ソフトベンダーへ調査依頼
- 事象に応じて自社の情報セキュリティ担当者より
  TCS-HD情報セキュリティ室へ報告
- 感染したコンピュータを再使用する場合
  - ウイルスが完全に駆除できたことを確認する
  - ウイルスが駆除できない場合はPCの初期化インストールを実施

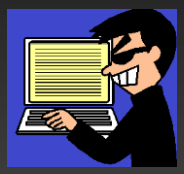
ウイルスに感染した疑いを持った場合、次の対処を行ってください。

・直ちにネットワークから切断し、PCを隔離する。有線LANはLANケーブルを抜き、無線LANは無線設定から切断する。
また社給スマホでUSBテザリングしている場合は、USBケーブルを抜く。
・周囲の人へも事象を伝え、感染が拡散していないか確認する。
・自社の情報セキュリティ担当者またはシステム管理者へ感染時の状況（PCの挙動や症状、感染日時など）を報告し指示を仰ぐ。
・疑いのあるPCに対して、手動によるウイルス検索を行う。
・手動によるウイルス検索で検知できない場合は、自社の情報セキュリティ担当者またはシステム管理者と相談し、ウイルス対策ソフトベンダーへ調査を依頼する。

なお、発生した事象に応じて自社の情報セキュリティ担当者よりTCS－HD情報セキュリティ室へ報告をしてください。
ウイルス感染したPCを再使用する場合は、ウイルスが完全に駆除できたことを確認後、使用してください。
尚、ウイルスが駆除できない場合は、PCの初期化インストールを実施してください。

公衆無線LAN利用時の注意

- **公衆無線LANの利用リスク**
  - 公衆無線LANはどこでも使えて便利だが、悪意ある人に悪用される可能性がある
  - 悪意ある人が偽のアクセスポイントに、なりすましている事がある
- **無線LANを使用する際の注意**
  - **適切に管理、運用されていない公衆無線LANの設置、使用はルール違反！**
  - **ガイドラインに従い適切な構築、管理運用すること**
  - **社給デバイスでフリースポットに接続しない事！**
  - **無線LANに自動的に接続しない設定になっているかを確認！**



公衆無線LAN利用には多くのリスクが伴います。セキュリティ対策が不十分な場合、悪意ある第三者に悪用される可能性があります。

例えば、偽のアクセスポイントを介してデータが盗まれたり破壊されたりするリスクがあります。

適切に管理・運用されていない公衆無線LANの設置や使用はルール違反となります。

さらに、PCだけでなく、社給スマホなどのデバイスもフリースポットに接続することは禁止されています。情報漏えいやウイルス感染の危険性があるためです。

無線LANに自動的に接続しない設定を確認し、通常は通信設定をオフにしておくことを推奨します。

画面は自動で切り替わります

残り [redacted]

設問3

社給スマホに関する文章のうち、不適切なものをすべて選択しなさい。

1. 開発画面情報を顧客未許可の社給スマホで撮影して、社内メンバーにメールで問い合わせた。

2. 在宅勤務中、業務用PCの調子が悪いため、顧客未許可の社給スマホでWeb会議に参加した。

3. お客様も業務用スマホでWeb会議に参加しているので、許可を得ていないが自社の社給スマホでWeb会議に参加した。

TCS GROUP

設問3　社給スマホに関する文章のうち、不適切なものをすべて選択しなさい。

1. 開発画面情報を、顧客未許可の社給スマホで撮影して、社内メンバーにメールで問い合わせた。

2. 在宅勤務中、業務用PCの調子が悪いため、顧客未許可の社給スマホでWeb会議に参加した。

3. お客様も業務用スマホでWeb会議に参加しているので、許可を得ていないが自社の社給スマホでWeb会議に参加した。

画面は自動で切り替わります

残り [redacted]

設問4

在宅勤務に関する文章のうち、不適切なものを選択しなさい。

1. 社給PCと社給スマホをUSBケーブルで接続し、社給スマホは自宅の無線LANに接続して業務を行った。
2. 在宅勤務を行うためPCを持ち帰る際、バッグを持っているのが大変だったので網棚に置いた。
3. 顧客の許可を得た上で顧客貸与PCを自宅ネットワークに直接接続してWeb会議に参加していた。

TCS GROUP

設問4　在宅勤務に関する文章のうち、不適切なものを選択しなさい。

1. 社給PCと社給スマホをUSBケーブルで接続し、社給スマホは自宅の無線LANに接続して業務を行った。
2. 在宅勤務を行うためPCを持ち帰る際、バッグを持っているのが大変だったので網棚に置いた。
3. 顧客の許可を得た上で顧客貸与PCを自宅ネットワークに直接接続してWeb会議に参加していた。

画面は自動で切り替わります

残り [redacted]

設問5

コンピュータウイルスに関する文章のうち、不適切なものを選択しなさい。

1. ウイルス感染したことを自社の情報セキュリティ担当者に報告し、指示を仰いだ。
2. ウイルス感染に気が付いたため、周りに言わずにすぐ自分のPCのみ手動でウイルス検索を実施した。
3. 感染したPCについて、初動対策完了後、初期化インストールしてから、自社ネットワークに接続した。

TCS GROUP

設問5　コンピュータウイルスに関する文章のうち、不適切なものを選択しなさい。

1. ウイルス感染したことを自社の情報セキュリティ担当者に報告し、指示を仰いだ。
2. ウイルス感染に気が付いたため、周りに言わずにすぐ自分のPCのみ手動でウイルス検索を実施した。
3. 感染したPCについて、初動対策完了後、初期化インストールしてから、自社ネットワークに接続した。

5. 各種ツール利用の注意

第5章 「各種ツール利用の注意」

メール利用時の注意

- **メールからのウイルス感染事例**
  - 見知らぬアドレスから届いたメールを安易に開いた。
  - メールソフトのプレビュー機能を有効にしていた
  - 添付ファイルを安易にダウンロードした。
  - メール本文に記載されているURLを安易にクリックした。

- **ウイルスに感染しないための対策**
  - 身に覚えのないメール、心当たりのないメールは開かない。
  - メールソフトのプレビュー機能は無効にしておく。
  - 添付されたファイルを安易にダウンロードしない。
  - メール本文に記載されたURLを無暗にクリックしない。

メール利用に伴う情報セキュリティ事故は毎年発生しています。
メール誤送信による情報漏えいや、ウイルス感染によるデータの改ざん。
さらに、ウイルス感染したPCを踏み台にし、他のPCにウイルスを感染させてしまうリスクが発生します。
ここでは、メール利用に伴う注意事項と対策について説明します。

まず、メールからウイルスに感染する注意事項と対策について説明します。
ケースとして以下の原因が挙げられます。
・見知らぬアドレスから届いたメールを安易に開いた。
・メールソフトのプレビュー機能を有効にしていた。
・添付ファイルを安易にダウンロードした。
・メール本文に記載されているURLを安易にクリックした。

対策として、
・見知らぬアドレスから届いたメール、身に覚えのないメールは安易に開かない。
・メール本文のプレビューによるウイルス感染を防ぐため、メールソフトのプレビュー機能を無効にする。
・添付ファイルによるウイルス感染を防ぐため、添付ファイルを安易にダウンロードしない。
・悪意のあるサイトからのウイルス感染を防ぐため、URLを無闇にクリックしない。
・OSやソフトウェアの脆弱性によるウイルス感染を防ぐため、OSやソフトウェアのアップデートは必ず実施する。

これらの点に十分注意し、メール利用におけるウイルス感染予防に努めてください。

5. 各種ツール利用の注意

メール利用時の注意

- **メールの誤送信の事例**
  - 送信前の宛先確認が不十分
  - 初めてメールをする相手のメールアドレスの確認不足
  - 宛先を確認しないまま、安易に全員に返信
  - 送信相手は正しかったが、添付するファイルが誤っていた

- **メールの誤送信対策**
  - メール送信前に必ず送信相手のアドレス、名前、会社名を確認する
  - 誤送信対策機能を活用して、氏名、アドレスの確認を行ってから送信する
  - 初めて送信する相手には、名刺のアドレス、送信前に電話確認などを行う
  - 同姓の宛先誤り防止のために、アドレス帳の登録名を区別する
  - アドレスだけではなく、アットマーク以降のドメインも確認

次にメール誤送信についての注意事項と対策について説明します。

ケースとして以下の原因が挙げられます。
・送信前の宛先確認が不十分。
・初めてメールをする相手のメールアドレスの確認不足。
・宛先を確認しないまま、安易に全員返信。
・添付ファイルの誤り。

メールの誤送信対策として、
・メール送信をする前に必ず送信相手のメールアドレス、名前、会社名を確認してください。
確認するための方法として以下が挙げられます。
・メールソフトの誤送信対策機能である誤送信対策機能を活用し、氏名、アドレスの確認後、送信する。
・初めてメールをする相手には、名刺に記載されているメールアドレスを確認してから送信する。
又は、直接本人に電話してメールアドレスの確認をしてから送信する。
・同姓の宛先設定誤りを防ぐため、アドレス帳の登録名を区別できるよう氏名の前に会社名を付けるなど適宜見直しを行う。
・一斉送信や全員返信の場合、送信相手に他者のメールアドレスが参照されないようにBCCに宛先を設定する。

5. 各種ツール利用の注意

メール利用の注意

- **ファイルを誤って添付しないための対策**
  - 情報漏えいの低減のため、安易にファイル添付をしない。
  - 添付するファイルの名前だけで判断せずに、ファイルの中身を確認する。
  - 不要な機密情報等が含まれていないか、ファイルの中身を確認する。
  - 誤送信対策機能で保留された、添付ファイルの中身を必ず確認する。

次に添付ファイル誤りの対策として、

・情報漏えいの低減のため、安易にファイル添付をしない。
・添付するファイルの名前だけで判断せずに、ファイルの中身を確認する。
・添付するファイルに不要な個人情報や機密情報が含まれていないか、ファイルの中身を確認する。
・誤送信対策機能の保留通知の添付ファイルも必ず開いて、ファイルの中身を確認する。

メールを誤送信すると機密情報が漏えいする恐れがあるだけではなく、メールアドレス等個人情報も漏えいしてしまうことになります。また、宛先誤りによる情報漏えい防止策として、メールにファイルを添付するのではなく、外部クラウドストレージに保存する方法も有効です。

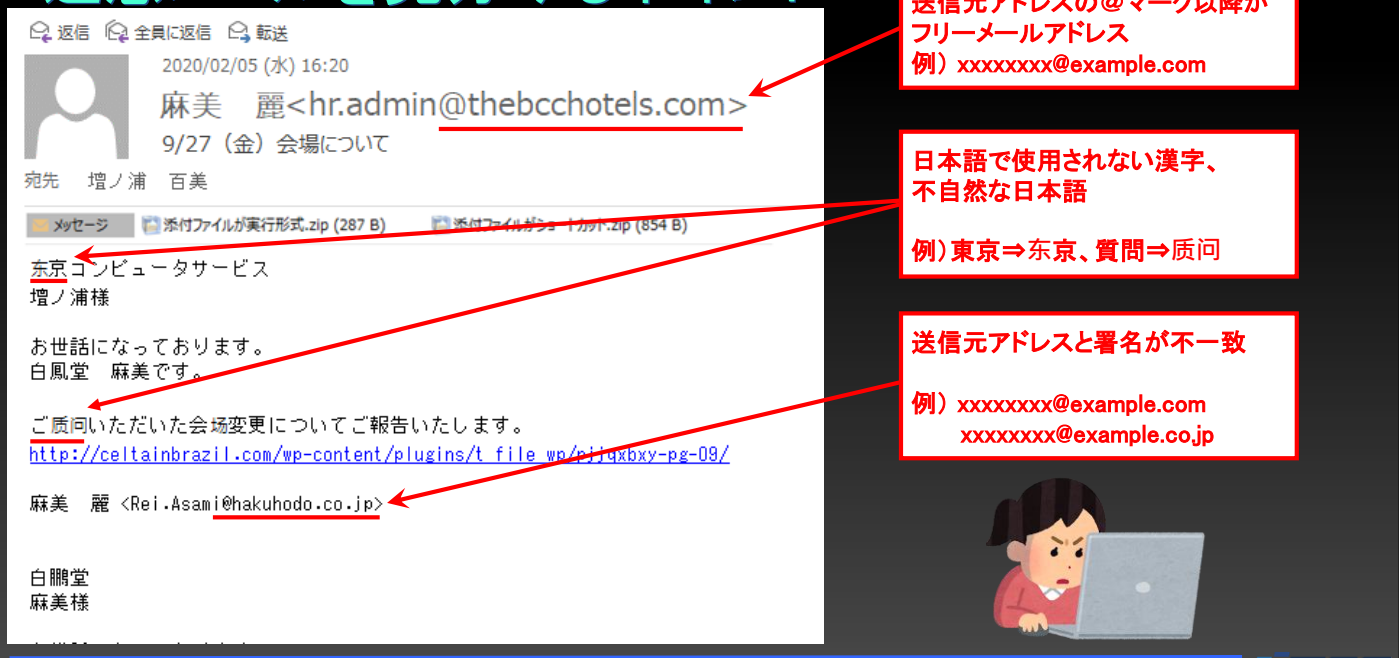
メールにはファイルのリンクのみを記載して、本来の送信相手はリンク先から、あらかじめ通知されている開封パスワードでファイルを参照します。一方、宛先誤りによる送信相手は、開封パスワードを知らされていないため、ファイルを参照することが出来ません。本対策により、情報漏えいが低減します。

漏えい事故を起こしてしまうと会社の信用を落とし、業績の低下に繋がります。最悪の場合、謝罪だけでは済まされず、顧客との契約解除、損害賠償請求、警察庁に調査される事や、マスコミによる社名公開など行われるケースもあります。

特に急いでいる時や多忙な時こそ、メールの送信は慎重に行ってください。

5. 各種ツール利用の注意

迷惑メールを見分けるポイント



迷惑メールは、受信者に興味を持たせ、本文中のURLや添付ファイルを開かせようとします。メールによる情報セキュリティ事故にあわないために、普段から受信したメールが迷惑メールではないか注意を払う必要があります。

また、迷惑メールが届く原因として、信用出来ないサイトへのアクセスやメールアドレスの登録、SNS上への電話番号やメールアドレスの登録などが挙げられます。業務に関係のないサイトやSNSのアクセスは禁止です。

ここでは、【迷惑メールを見分けるポイント】を押さえ、被害にあわないようにしてください。

【迷惑メールを見分けるポイント】

送信元アドレスの＠以降がフリーメールのドメインである。

送信元アドレスが似ているが、公表されているアドレスと異なる(例：正：amazon　偽：amazone　等)

送信元の組織名や電話番号をメール以外の情報源から調べても実在しない。

日本語では使用されない漢字が使われていたり、不自然な日本語となっている。

送信元アドレスとメールの署名が異なる。

5. 各種ツール利用の注意

迷惑メールを見分けるポイント

返信　全員に返信　転送

2020/02/05 (水) 16:20

麻美　麗<hr.admin@thebechotels.com>

9/27（金）会場について

宛先　壇ノ浦　百美

メッセージ　添付ファイルが実行形式.zip (287 B)　添付ファイルがショートカット.zip (854 B)

东京コンピュータサービス
壇ノ浦様

お世話になっております。
白鳳堂　麻美です。

ご質問いただいた会場変更についてご報告いたします。
http://celtainbrazil.com/wp-content/plugins/t_file_wp/pjjqxbxy-pg-09/

麻美　麗 <Rei.Asami@hakuhodo.co.jp>

白鵬堂
麻美様

件名と送信のタイミングが不自然

添付ファイルが実行形式
（開封すると、実行されるexeファイル）

不審なURL

件名とメールが送信されているタイミングが不自然である。
簡単な英語の本文が記載されている。
本文中に表示されているURLと、リンク箇所にマウスカーソルを当てた際に表示されるURLが異なる。
添付ファイルの拡張子がexe、scr、cplといった実行形式のファイルである。
データファイルであってもOSやアプリケーションの脆弱性を悪用してウイルス感染させるものもあります。
添付ファイルがショートカットファイルである。アイコンの左下に「矢印のマーク」がある。
まずは、目視確認を行うことを心掛けてください。

迷惑メールを見分けるポイント

- **フィッシングメールとは**

入力者の認証情報やクレジットカード情報、個人情報などを
盗み取る目的で不特定多数に送信されてくるメールのこと。

URLが記載されており、このフィッシングサイトで情報を入力すると
情報が盗まれて悪用される可能性があります。

フィッシングメールとは

入力者の認証情報やクレジットカード情報、個人情報などを盗み取る目的で不特定多数に送信されてくるメールのことです。

このメールには、公的機関や金融機関、ショッピングサイト、宅配業者等の有名企業のサイトを模倣して入力情報を盗む目的の偽の

ウェブサイトへ誘導するURLが記載されており、このフィッシングサイトで情報を入力すると情報が盗まれます。

5. 各種ツール利用の注意

＜ご参考：フィッシングに関する注意喚起＞

●IPA　独立行政法人　情報処理推進機構【ビジネスメール詐欺 事例集】
https://www.ipa.go.jp/security/bec/bec_cases.html

●警察庁　フィッシング対策
https://www.npa.go.jp/bureau/cyber/countermeasures/phishing.html

●総務省　総務省を騙るフィッシングサイトに関する注意喚起
https://www.soumu.go.jp/menu_kyotsuu/important/kinkyu02_000511.html

●厚生労働省　厚生労働省を名乗るフィッシングサイトへの注意喚起について
https://www.mhlw.go.jp/stf/newpage_32266.html

参考までに、フィッシングメールの対応について、サイト上で各機関から注意喚起をしています。今一度内容を確認し、ウイルス感染リスクを減らしましょう。

＜ご参考：フィッシングに関する注意喚起＞

●IPA　独立行政法人　情報処理推進機構【ビジネスメール詐欺 事例集】
https://www.ipa.go.jp/security/bec/bec_cases.html

●警察庁　フィッシング対策
https://www.npa.go.jp/bureau/cyber/countermeasures/phishing.html

●総務省　総務省を騙るフィッシングサイトに関する注意喚起
https://www.soumu.go.jp/menu_kyotsuu/important/kinkyu02_000511.html

●厚生労働省　厚生労働省を名乗るフィッシングサイトへの注意喚起について
https://www.mhlw.go.jp/stf/newpage_32266.html

5. 各種ツール利用の注意

チャットツール

- **チャット利用時の注意事項**
  - ➢ 社外のメンバーがいるチャットに、機密情報を書いてしまった。
  - ➢ 個人情報が記載されたデータを、パスワードを掛けずに送ってしまった。
  - ➢ 誤って、違うチャットルームに個人情報、機密情報を投稿してしまった。
  - ➢ 同姓同名の方を、誤ってグループに招待してしまった。
  - ➢ 同姓同名の方に、誤って機密情報をチャットで送信してしまった。

  チャットの送信、グループへの追加の際は必ず相手の氏名、または社員番号を確認してから行ってください。



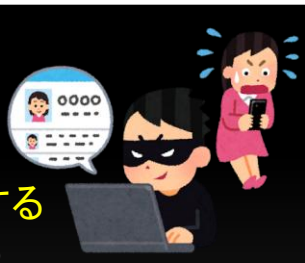
チャットツールはコミュニケーションの活発化、業務の効率化など利便性が高い一方で、情報漏えいなどセキュリティリスクが存在することを注意してください。

手軽に素早くコミュニケーションが取れて、情報の共有が簡潔にできます。
グループチャットでは簡単に複数人による打ち合わせができて、対面である必要もありません。
やり取りが手軽な分、スピード感重視で利用する傾向があるため情報セキュリティ意識が希薄になりがちです。
例えば、
・グループメンバー追加時に、同姓同名の違う方を追加してしまった。
・社外のメンバーがいるグループチャット内で機密情報を書きこむ。
・個人情報を含むデータをパスワードもかけずにグループチャットで送る。
・チャット内に書き込まれた何気ないURLをクリックしてみる。
・簡単な内容なので取りあえず返信しておく。
・送られてきたものは取りあえず中身を確認してみる。
・違うチャットルームに投稿してしまった。

など本人にとっては何気ない判断かもしれませんが、重大な情報セキュリティ事故を簡単に発生させてしまうのがチャットツールです。
コミュニケーションを行う上でやり取りのハードルが下がった分、これまで以上にリスクがないか意識して注意する必要があります。

5. 各種ツール利用の注意

私的SNSアカウントの投稿



- **SNS投稿に潜むリスク**
  - 文章、画像、映像などから機密情報、個人情報が漏えいする
  - 著作権や肖像権を含む投稿を行い、権利を侵害してしまう
  - 個人名、企業名、所属、職務内容を安易に投稿して、社会的信用を失う
  - 不確かな情報を無暗に投稿して、虚偽の情報を流布してしまう

- **投稿時の注意点**
  - 機密情報、個人情報を含む文書、画像、映像、発言、投稿は厳禁
  - 著作権や肖像権を含む投稿は極力、控える
  - 個人名、企業名、所属、職務内容など特定に繋がる情報は除外する
  - 事実に反する内容、不快感、嫌悪感を抱かせるような発信は控える

ソーシャルネットワークサービス（SNS）は、インターネットを通じて人と人をつなげるサービスです。

例えば、Facebook、Instagram、Twitter（現在のX）、LINEなどが有名です。サービスの利用者が情報を発信して、発信された情報がインターネット上で形成されていきます。

実名、匿名どちらでも手軽に発信できるという利便性がありますが、その反面、熟考することなく不用意に発信してしまう事が多く、一度発信してしまうと、インターネットやその他の情報通信を通じて、急速に拡散され続けるおそれがあります。

SNSを利用する際は、不用意な発言に十分な注意を払ってから発信してください。

不用意な発言がきっかけとなって、他の利用者から非難などを浴びることになると、その影響は投稿者本人の所属する企業や組織にまで及び、企業のブランドイメージを損なうリスクがあります。

・機密情報、個人情報を含む発言、発信、画像の投稿は行わない。
・発信する内容が著作権や肖像権の侵害に該当しないように確認を行う。
・発信した内容から、個人、企業、所属、場所などが容易に特定されるような情報は除外する。
・事実に反する内容、他人に不快感、嫌悪感を抱かせるような不適切な発信は行わない。
・第三者にアカウントを乗っ取られないように、アカウント情報の適切な管理を行う。
・利用するサービスの規約を遵守する。

何気ない発信が原因となって、大きなトラブルに発展するリスクがあることを十分に理解してください。

Web会議の使い方

Jitsi Meet

- **注意事項全般**
  - 第三者へ機密情報がもれないよう配慮する。
  - 個人情報の取り扱いに注意する。
  - 公共の場所でのWeb会議の利用は禁止する。
  - 外部のクラウド上へ録画ファイルを置かないこと。
- 主催する場合
  - 会議参加者の出席確認を実施する。
  - 会議には招待した特定の人以外参加できないようにする。
    - 対策の例
      パスワードの設定、待合室の利用、会議室のロック、強制退室など
- 招待される場合
  - 招待されたURL/会議室番号等が信頼できる発行元か確認する。

リモートワークを筆頭に日常的にWeb会議を利用しています。
当たり前のように利用しているWeb会議ですが、利用する際の注意点は守っていますか？

- 会議中は第三者へ情報がもれないよう配慮する。
- 社内の機密情報について発言しない。
- 個人情報の取り扱いに注意する。

カフェ、電車などの公共の場所では他人に画面をのぞかれ会議内容が漏えいするリスクがあるため、Web会議の利用は禁止です。
さらに、外部のクラウド上へWeb会議の録画ファイルを置かないでください。

Web会議を主催する場合、会議室のURLを使いまわすことがあると思います。特に定期的に開催する会議の場合はその傾向が強くなります。
同じURLを使いまわすことで万が一このURLが外部に漏れた場合は不正アクセスの一因となる可能性があるため、使いまわしはやめてください。
さらに、会議参加者の出席確認を実施してください。
会議には招待した特定の人以外は、参加できないように対策することも重要です。
対策例としては以下の方法が考えられますので、最低一つ以上は実施してください。

- 会議室にはパスワードをかける。
- 待合室機能がある場合は積極的に利用する。
- 会議開催中に予期しない人が参加しないようロックする。
- 会議開催中に予期しない人が参加して来た場合、強制的に退室させる。

また、Web会議に招待された場合、招待されたURL/会議室番号等が信頼できる発行元か確認してください。

5. 各種ツール利用の注意

生成AIの注意点

- **生成AIの注意点**
  - ➢ 内部からの情報漏えいリスク

    AIに対して機密情報、個人情報を入力する際は、十分に検討してください。
    情報の漏えいは、社会的信用の失墜、企業価値の損失に繋がります。

  - ➢ 誤った生成への対策

    高度な専門知識を要する質問に対して、誤った内容が生成される可能性があります。
    生成された内容をそのまま流用すると、思わぬトラブルに発展するリスクがある。

  - ➢ 権利侵害への対策

    生成された内容がすべてオリジナルではない事を意識してください。
    侵害リスクを完全に防ぐのは難しいため、生成されたコンテンツが既存の著作物に酷似していないかを確認するプロセスを設けることも必要です。

Twitter（現在のX）は、2024年12月から有料サービスの生成AI、Grok（グロック）が実装されました。

今後、様々なSNSや生成AIの導入が予想されます。生成AIのサービスを利用する場合、どのような問題点やリスクを意識すればよいのでしょうか。

・内部からの情報漏えいリスク

利用者が入力したデータをAIは学習します。生成AIの種類によっては、学習したデータを再利用するものもあります。そのため、AIに対して企業の機密情報、個人情報を入力すると、入力した情報が第三者への回答や生成などに使用される情報漏えいリスクがあります。

・誤った情報が生成されるリスク

AIの学習ボリュームが少ない話題、高度な専門知識を要する質問に対して、誤った内容が生成される可能性があります。事実に基づかない、でたらめな生成を行ってしまう現象をHallucination（ハルシネーション）と言い、生成された内容をそのまま流用してしまうと、思わぬトラブルに発展してしまうリスクがあります。

・知的財産権などの侵害リスク

AIから生成されるものには、すでに存在する作品や作風と似通ったものが生成される可能性があります。たとえば、すでに存在する画像と著しく類似している。存在する作品を模して生成されている特徴がある場合、生成されたデータを公表、販売、展示、配信などを行うと権利を侵害してしまう可能性があります。侵害リスクを完全に防ぐのは難しいため、生成されたコンテンツが既存の著作物に酷似していないかを確認するプロセスを設けることも必要です。

AIの最大の特徴は学習機能を持つことです。対策としてAIを利用する場合には以下の点に注意してください。

・利用規約に入力された内容を学習データには使用しないと明記されているか確認する。

・入力された情報が適切に保護されることが利用規約に明記されているか確認する。

・生成AIの学習機能を利用者側で無効にする設定が備わっているAIであるか確認する。

画面は自動で切り替わります

残り [redacted]

設問6

メールの誤送信対策の行動として不適切なものを選択しなさい。

1. メール誤送信対策機能から自動返信された内容は宛先、件名、本文、添付ファイル名、添付ファイルの内容を必ず指差し確認をしてから、メールの送信を行っている。
2. 身に覚えがないメールが届いた時、上長、部門長、メンバーに報告のみ行ってメールの開封はしていない。
3. メールの宛先間違いに気づいたが、誤って送った相手からメールを消した連絡があったので、そのまま業務を続けた。

TCS GROUP

設問6　メールの誤送信対策の行動として不適切なものを選択しなさい。

1. メール誤送信対策機能から自動返信された内容は宛先、件名、本文、添付ファイル名、添付ファイルの内容を必ず指差し確認をしてから、メールの送信を行っている。

2. 身に覚えがないメールが届いた時、上長、部門長、メンバーに報告のみ行ってメールの開封はしていない。

3. メールの宛先間違いに気づいたが、誤って送った相手からメールを消した連絡があったので、そのまま業務を続けた。

画面は自動で切り替わります

残り [redacted]

設問7

SNSを利用する際の行動として適切なものを選択しなさい。

1. 職場の先輩が公開前の製品情報を教えてくれたので、SNSアカウントで製品情報を投稿した。
2. プロジェクトの打ち上げ終了後、メンバーと記念撮影をしてSNSに画像つきで投稿した。
3. 著名人のスキャンダルや災害情報などを見かけても、投稿内容を確認してから発信するか判断している。

TCS GROUP

設問7　SNSを利用する際の行動として適切なものを選択しなさい。

1. 職場の先輩が公開前の製品情報を教えてくれたので、SNSアカウントで製品情報を投稿した。
2. プロジェクトの打ち上げ終了後、メンバーと記念撮影をしてSNSに画像つきで投稿した。
3. 著名人のスキャンダルや災害情報などを見かけても、投稿内容を確認してから発信するか判断している。

画面は自動で切り替わります

残り [redacted]

設問8

生成AI利用時の注意事項として適切なものを選択しなさい。

1. 生成AIの回答は常に進化しているので、内容の確認をする必要はない。
2. 生成された画像や映像はオリジナルなので、著作権や肖像権を気にする必要はない。
3. 生成された内容を使用する前に、生成内容を周りの人や有識者に相談している。

TCS GROUP

設問8　生成AI利用時の注意事項として適切なものを選択しなさい。

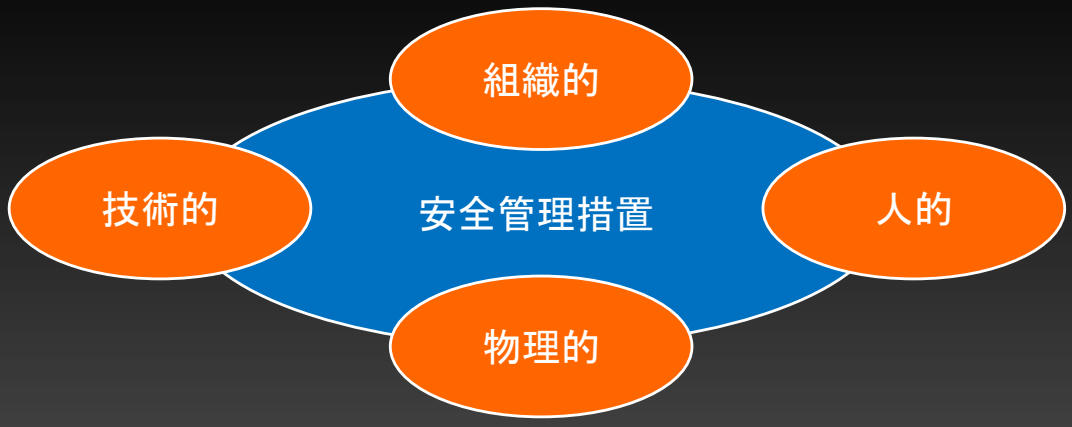
1. 生成AIの回答は常に進化しているので、内容の確認をする必要はない。
2. 生成された画像や映像はオリジナルなので、著作権や肖像権を気にする必要はない。
3. 生成された内容を使用する前に、生成内容を周りの人や有識者に相談している。

6. 個人情報保護

第6章 「個人情報保護」

個人情報を守るために必要なこと

個人情報保護法では、「4つの視点」からの安全管理措置を義務付けています



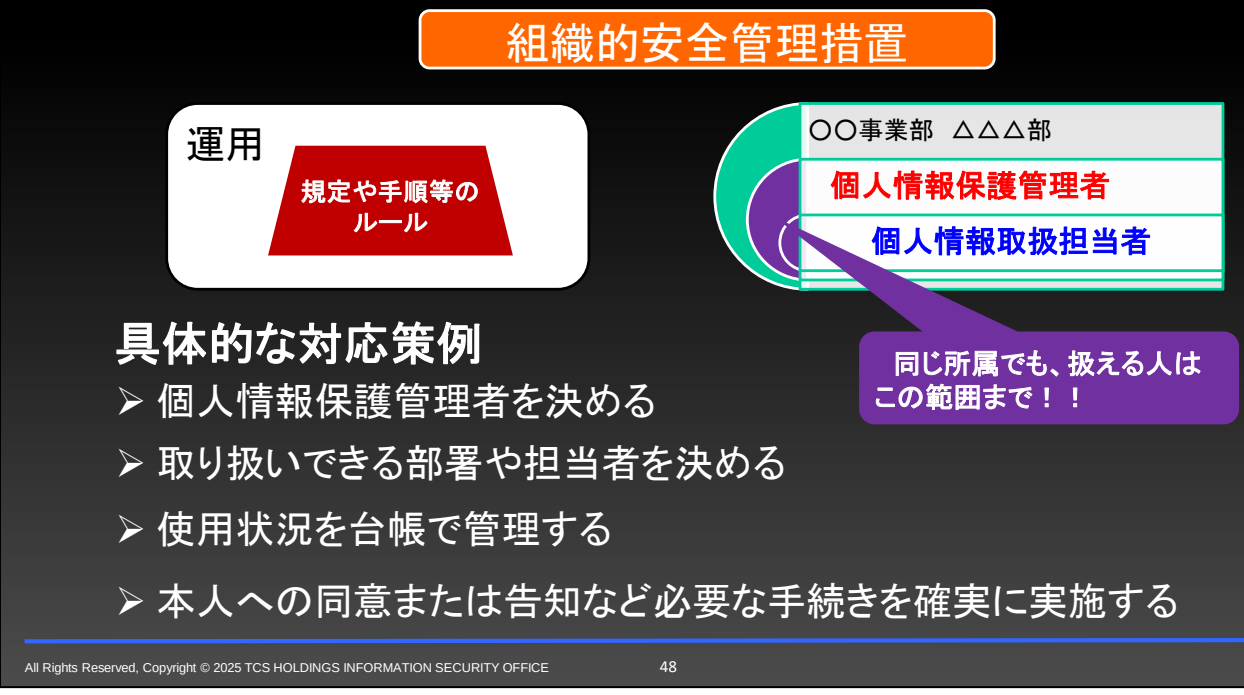
個人情報保護のために、個人情報を扱う場合、「安全管理措置」を実施することが個人情報保護法で義務付けられています。

具体的には「組織的」「人的」「物理的」「技術的」の4つの視点から安全管理措置を講じなければなりません。

そして、定期的に活動内容の評価、見直し、改善を行い、永続的な管理の仕組みを構築して、実効性を高めていくことが重要です。

「大丈夫だろう」ではなく「情報漏えいを発生させない」ことを目標に、具体的な対策を実施することが重要です。

個人情報を守るために必要なこと



具体的な対応策例

- 個人情報保護管理者を決める
- 取り扱いできる部署や担当者を決める
- 使用状況を台帳で管理する
- 本人への同意または告知など必要な手続きを確実に実施する

はじめに、個人情報を扱う事業者は、安全管理について社員の責任と権限を明確に定め、安全管理に対する規定や手順書を整備運用し、その実施状況を確認する必要があります。

個人情報を扱う事業者が実施する組織的安全管理措置の具体的な対応策例として、次のようなことが挙げられます。

個人情報保護管理者を決める。

個人情報を取扱う部署や作業担当者を決める。

取扱状況を一覧できる台帳で管理する。

利用にあたっては本人への同意または告知など必要な手続きを確実に実施する。

ルールに沿った適正な管理を実施していくことが重要です。

個人情報を守るために必要なこと

人的安全管理措置

秘密保持誓約書を提出

秘 密 保 持 誓 約 書

年　　月　　日

××××××××××株式会社

代表取締役社長　　●●　　▲▲　殿

住　所:＿＿＿＿＿＿＿＿＿＿＿＿

氏　名:＿＿＿＿＿＿＿＿＿＿＿＿印

私は、××××××××××株式会社（以下「当社」という）入社に際し当社の一員として、下記の事項を遵守することを誓約いたします。

私は、下記の事項に違反し、当社に重大な損害を与えた場合は、当社規定に則り、損害賠償請求、刑事告訴及び人事・労務上等 いかなる処分を受けても異議はありません。

個人情報を守れるかどうかは、この仕組みを動かす人そのものにかかっています。
そのために、個人情報を扱う事業者は、人的安全管理措置として、皆さんが業務で知った情報を在職中も退職後も、漏えいしないように秘密保持誓約書を提出してもらっています。
同様のことを外部委託先にも守ってもらうように書面を取り交わすことになっています。

書面の取交しだけでなく、継続してルールが守られ情報が漏えいしないために、社員の皆さんに対する情報セキュリティ教育の実施も必要となります。

個人情報を守るために必要なこと

物理的安全管理措置

具体的な対応策例

- 個人情報の保管場所を明確化し、分離した場所として区分けをする
- 保管場所はキャビネット等、施錠ができる場所で行い、鍵は個人情報の管理者が管理する

誰もが容易に個人情報を閲覧でき、持ち出せるようでは、紛失や漏えい事故が発生しかねません。

個人情報を扱う事業者が実施する物理的安全管理措置の具体的な対応策例として、次のようなことが挙げられます。

他の情報とは分離して保管する。

保管場所は施錠できる場所にする。

個人情報保護のためには、物理的に保護された室内で個人情報を使用し、管理することが重要です。

個人情報を守るために必要なこと

技術的安全管理措置

具体的な対応策例

- アクセス権限を個人毎に決め、許可された人だけがアクセスできるようにする
- アクセスログをとり、不正なアクセスがないかチェックする
- データを暗号化し、機密性を確保する
- 不正侵入等の攻撃から、自社のネットワークを防御する

最後に、個人情報を扱う事業者が実施する技術的安全管理措置の、具体的な対応策例をご紹介します。
アクセス権限を個人毎に決め、許可された人だけがアクセスできるようにする。
アクセスの記録を取る
データを暗号化し機密性を確保するなどがあります。
このような保護を行い、個人情報を守っていくことが重要です。

マイナンバー（個人番号）制度

■マイナンバーって何のこと？

▷ マイナンバーは通称で、正式名称は「個人番号」。
国内のすべての住民に指定・通知されている12桁の番号のこと。
※ マイナンバー制度は2016年1月に開始。
原則としてマイナンバーは、生涯同じ番号を使用します。

■どーしてマイナンバーが必要なのか？

▷ 「社会保障」「税」「災害対策」の3つの分野で、それぞれの機関に存在する個人の情報が、同一人の情報であることの確認に利用するため。

2016年1月から、国民一人ひとりが1つの番号で行政サービスを受けられる「マイナンバー制度」が導入されました。

マイナンバーは通称で、正式名称は個人番号といい、生涯にわたって利用する番号です。

ではマイナンバーは何に使うのでしょう。

それは「社会保障」「税」「災害対策」の分野で、それぞれの機関に存在する個人の情報が、同一人の情報であることの確認に利用するためです。

マイナンバー（個人番号）制度

■会社が社員のマイナンバーを収集するのはなぜ？

▷ 社会保障手続き（厚生年金・健康保険・雇用保険）
→年金事務所や健康保険組合へ提出

▷ 税金手続き（源泉徴収票の作成・年末調整の手続き）
→税務署へ提出

■マイナンバーが漏えいしたらどーなる？

▷ あらゆる公共機関で個人情報にアクセスできるパスワードのようなもの。悪用されて、持ち主の権利や利益が危うくなる！！

会社がなぜマイナンバーを収集するのか。それは、主に「社会保障」「税」の分野で利用するためです。
その具体的な利用場面は、
　出産育児一時金の申請や育児休業の申請、雇用保険、年金など、社会保障の手続き。
　年末調整で提出する扶養控除等申告書など、税金の手続き。
が挙げられます。

では、マイナンバーが漏えいしてしまったらどうなるのでしょうか。
マイナンバーは一人ひとりに対してたった一つしか与えられない番号です。言ってみれば、あらゆる公共機関で個人情報にアクセスできるパスワードのようなもの。
金融や医療分野にも利用範囲を広げることも想定されているため、その重要性はさらに増すと考えられます。
万が一にでも漏えいさせてしまうと、たちまちそのマイナンバーの持ち主の権利・利益が危うくなります。

マイナンバー（個人番号）制度

■不正利用が目的で漏えいさせた場合の罰則

⇒　例：4年以下の懲役もしくは200万円以下の罰金又は併科。

■不正に取得した場合の罰則

⇒　例：3年以下の懲役または150万円以下の罰金。

安全管理措置を確実に実施し
TCSグループとしての責任を果たしましょう

そのため、厳重な保護措置と罰則が設けられています。
正当な理由もなく漏えいしても、不正な手段で取得しても罰が課されます。
このことから、機密度の大変高い情報であることを十分に理解してください。

安全管理措置を確実に実施し、そして個人情報をしっかり守っていくことで、TCSグループまた個人としての責任を果たしましょう。

画面は自動で切り替わります

残り [redacted]

設問9

マイナンバー制度に関して不適切なものを選択しなさい。

1. マイナンバーと個人番号は同じものである。

2. マイナンバーは定期的に変更される。

3. マイナンバーは「社会保障」「税」「災害対策」の分野で、それぞれの機関に存在する個人の情報が、同一人の情報であることの確認のために利用される。

TCS GROUP

設問9　マイナンバー制度に関して不適切なものを選択しなさい。
1. マイナンバーと個人番号は同じものである。
2. マイナンバーは定期的に変更される。
3. マイナンバーは「社会保障」「税」「災害対策」の分野で、それぞれの機関に存在する個人の情報が、
同一人の情報であることの確認のために利用される。

7. 内部不正

第7章 「内部不正」

内部不正による個人情報持出

・国内での内部不正発生事例

- NTT西日本の子会社にて元派遣社員が10年間で約900万件の個人情報を記録媒体に保存し、名簿業者などに流出させた。
- 株式会社ベネッセコーポレーションのグループ会社の委託先社員が記録媒体に個人情報をコピーし、流出させた。

・不正を承知で行うことは犯罪！

- 持ち出した技術を転用したり、データを売却をした場合「刑法」や「民法」で個人的にも責任を問われる。

ここでは内部不正について説明します。
まず、国内での内部不正発生事例です。

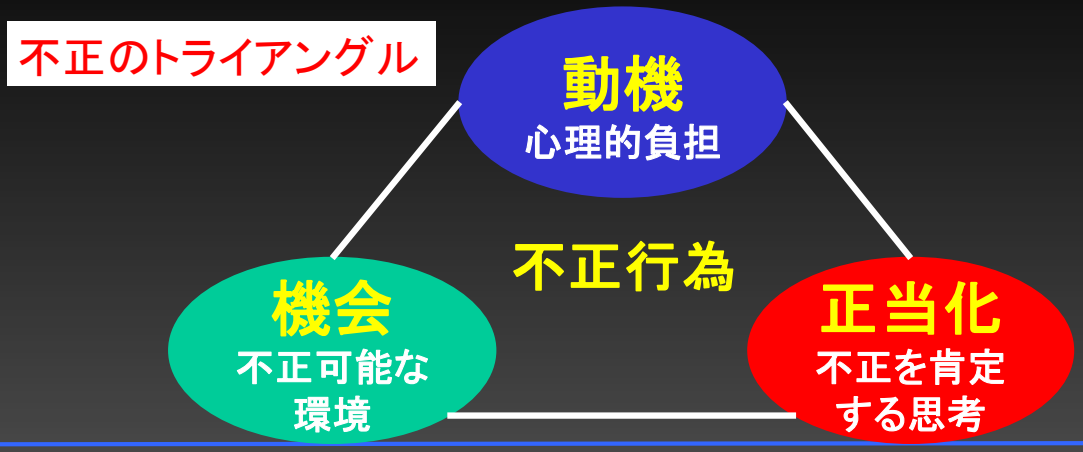
昨年10月、NTT西日本の子会社にてコールセンターシステムの運用保守を担当していた元派遣社員が、10年間で約900万件の個人情報を記録媒体に保存し、名簿業者などに流出させていました。

同様の内部不正の発生事例としては2014年7月、株式会社ベネッセコーポレーションの顧客データベースを保守管理するグループ会社の委託先社員が、記録媒体に個人情報をコピーし流出させたとして不正競争防止法違反の疑いで逮捕されました。

不正を承知で行うことは犯罪です。
持ち出した技術を転用したり、データを売却した場合、「刑法」や「民法」で個人的にも責任を問われることになります。

内部不正による個人情報持出しの問題点

・不正会計リスクや外部からのサイバー攻撃のリスクに比べ
内部不正のリスクは経営課題としての意識が薄い
- ➢ 内部不正対策として従業員に対する教育が必要



IPAによる「企業の内部不正防止体制に関する実態調査」によると、多くの企業では不正会計リスクや外部からのサイバー攻撃のリスクに比べ内部不正のリスクは経営課題としての意識が薄いとされており、内部不正対策として従業員に対する教育が必要である、とされています。

内部不正が起こる要因を分析した理論に「不正のトライアングル」があります。
不正のトライアングルの3つの要素がそろったとき、人は不正行為を働くとされています。

3つの要素の一つ目は「動機」です。
お金が必要、業務のノルマから逃げ出したい、などの心理的負担により、
会社の個人情報を持出し、売る、ノルマを達成したかのように見せかけるために粉飾するなどの内部不正につながります。

二つ目は「機会」です。
動機があっても不正を働くことが出来る機会、環境が無ければ内部不正を起こすことはできません。
しかし、チェックが形骸化している、重要な情報の管理を1人に任されているなどの不正可能な環境があると
内部不正を起こすことが可能となります。
在宅勤務の導入により、他の社員の目が無い環境で業務を行うことが多くなったため、内部不正の機会も増加しています。

三つ目は「正当化」です。
動機や機会があっても、多くの人は踏みとどまります。
普段からルールが形骸化し、破られているような状態では、心理的なハードルが下がり、
周りもやっているから自分もやって良いんだ、というような不正を肯定する思考が、不正行為につながります。

内部不正の対策

・権限の集中を防止する
- システム管理者等の特権操作に承認者を設ける。
- 特定の限られた人間だけでなく、別の人間もチェックを行う。

・不正操作のチェックを行う
- 電子メールや外部記録媒体での不正な持出しを行っていないかチェックを行う。
- 普段からアクセス履歴をログ管理して不正操作をチェックする。

・職場環境の整備をする
- 適正な労働環境や良好な職場内コミュニケーションを図り、組織への不満が起こらないようにする。

内部不正を防止するためには従来の機密情報の漏えい対策に加え、内部者に対しての備えが必要となります。

・権限の集中を防止する
システム管理者等の特権操作に承認者を設けるなど、権限の集中を防止する。
特定の限られた人間だけでなく別の人間もチェックを行う。
・不正操作のチェックを行う。
電子メールや外部記録媒体での不正な持ち出しを行っていないかチェックを行う。
また、普段からアクセス履歴をログ管理して不正操作をチェックすることも必要です。
・職場環境の整備をする。
適正な労働環境や良好な職場内コミュニケーションを図り、組織への不満が起こらないようにするなどといった対策を講じてください。

8. 事故発生時の対応

第8章 「事故発生時の対応」

8. 事故発生時の対応

報告ルートを前もって確認

・事故報告ルートは、解決に向けた情報共有と迅速な対応と解決が目的。

- 速やかに第一報を行うために、所属会社及び顧客先の報告ルートを必ず確認
- 情報セキュリティ事故の適切な対応が、信頼回復への第一歩
- 手帳に1次連絡先、2次連絡先等、複数の連絡先を控える

信頼回復

事故が発生したら、速やかに報告することが重要です。

そのためにも、社内および顧客先の事故報告ルートを、前もって確認してください。

その上で、確認内容を踏まえた、自分の事故報告ルートを作成してください。

また、担当者の異動により報告先が変わることもあります。報告ルートは定期的に見直してください。

報告ルートの不備が原因で、事故報告がリーダや営業担当者で止まるようなことがあると、顧客先から情報セキュリティ事故の隠蔽を疑われてしまいます。

また、情報セキュリティ事故の報告が正しく行われないことにより、拠点長や情報セキュリティ責任者がタイミングよくフォローアップを行うことができなくなる結果、情報セキュリティ事故へ適切に対応しない、と顧客先から疑われることにもつながります。

報告ルートは、顧客先、作業場所、プロジェクトなどの違いにより、報告先や報告順番が違います。

報告先の状況によっては、すぐに連絡が取れない場合もあります。迅速な報告を行うためにも手帳に1次連絡先、2次連絡先等、複数の連絡先を控えてください。

8. 事故発生時の対応

情報セキュリティ事故として取り扱う事項

事象	報告の対象例
①紛失・盗難	・ 入館証、セキュリティカード ・ 情報資産（電子媒体、紙媒体） ・ IT資産（社給PC、スマホ、タブレット）
②故意・過失	・ メール、Teams、郵便物の誤送信 ・ データの改ざん、データの削除 ・ セキュリティポリシーの違反
③攻撃	・ ウイルス感染 ・ 社内ネットワーク・インフラシステムへの無許可接続 ・ 可搬型記録媒体(USBメモリ、スマホ等)での情報資産の無許可持出し、無許可持込

情報セキュリティ事故として報告すべき対象事象を画面に表示します。

個人所有のスマホでも、顧客やTCSグループの方の連絡先、あるいは業務データが入っている場合は、機密情報の紛失、漏えいとして事故報告の対象になります。

また、社給スマホの一時的な紛失も事故報告の対象になります。コミュニケーションツール等の導入に伴い、事故報告対象も変化しています。

情報セキュリティ事故を起さないように、情報資産の取り扱いには常に注意してください。

8. 事故発生時の対応

まず、一報！

・事故が発生したら、直ぐに第一報を行う。

- 休日、夜間に関わらず、一刻も早く報告する
- 紛失した物を探し始める前に報告する
- 報告により、対処、指示を受ける

・報告ルート、連絡先を事前に確認しておく

- 各社の報告ルート、または顧客先での報告ルートを確認する
- 社給スマホのみに限らず、必要な連絡先は手帳等に必ず控える
- 事故が発生したら情報セキュリティ担当部署へ報告をする。

情報セキュリティ事故が発生した時、事故を認識したら、直ぐに第一報を行ってください。
例え休日、夜間でも、報告することが重要です。
第一報は情報セキュリティ事故を関係者が共有し、迅速に対処する事を目的としています。
紛失した物を探し始める前に、報告して、解決に向けた対処、指示を受けてください。

事故報告ルートの連絡先を社給スマホのみに登録している場合、社給スマホの紛失時に連絡先も同時に失います。
報告ルートを確認し、社給スマホを無くした時でも直ぐに報告ができるように、手帳等に連絡先を控えておいてください。
報告後は勝手な行動はせずに、必ず上司の指示を仰いでください。
また、事故が発生したら情報セキュリティ担当部署へ報告をしてください。

ヒヤリハットだからと言って安心してはダメ！！

・ヒヤリハットとは

大きな事故にならなかったが、ヒヤリとした、ハッとしたという危険を察知したときの心理状態を言います。

・ヒヤリハットが起きる原因

- 一時的な気の緩みや焦り
- 定期的な報告、連絡、相談不足
- 貸与物、ルールの確認不足
- 移動や業務の事前準備不足

ヒヤリハットとは大きな事故や事件につながらなかったものの、ヒヤリとした、ハッとしたという危険を察知したときの心理状態を表した言葉を組み合わせて、ヒヤリハットと呼びます。

ヒヤリハットが起きる原因として、以下があります。

・一時的な気の緩みや焦り
・定期的な報告、連絡、相談不足
・貸与物やルールの確認不足
・移動や業務の事前準備不足

ヒヤリハットは事故や事件につながる、一歩手前の危険な状況だったと認識してください。

ヒヤリハットを起した際に

・ヒヤリハットが起きた時の状況を分析して共有する

- ヒヤリハットがどのように起きたか状況を書き出す
- ヒヤリハットが起きた状況を、チームやメンバーと共有する
- 原因の特定と再発防止を実施する
- 大きな事故を起さないための予防策に繋げる

ヒヤリハットが発生してしまった時は、落ち着いて発生状況を紙に書きだしてみましょう。

文字にすることで、どのような状況でヒヤリハットが発生したのか、客観的に見ることができます。

ヒヤリとした、ハッとしたポイントに気付くことが事故の予防策にも繋がります。

運が良かった、事故にならなくて良かったと、ヒヤリハットをやり過ごしてしまうと、いつか大きな事故や事件につながります。

ヒヤリハットが発生した時の行動を振り返り、チームや部署内で情報共有を行い事故の予防策に活用してください。

画面は自動で切り替わります

残り [redacted]

設問10

情報セキュリティ事故発生時の対応として、適切なものを選択しなさい。

1. 出社時に入館証を紛失している事に気が付いた、急いで取りに帰り、無事自宅で見つかった。

2. 居酒屋で飲酒し、帰宅後に社給スマホがないことに気づいたが時間も遅いこともあり連絡が取れないと考え、翌日朝一番に報告した。

3. ヒヤリハットが発生してしまったため、チームで原因を分析し、対策を運用することにした。

TCS GROUP

設問10　情報セキュリティ事故発生時の対応として、適切なものを選択しなさい。

1. 出社時に入館証を紛失している事に気が付いた、急いで取りに帰り、無事自宅で見つかった。

2. 居酒屋で飲酒し、帰宅後に社給スマホがないことに気づいたが時間も遅いこともあり連絡が取れないと考え、翌日朝一番に報告した。

3. ヒヤリハットが発生してしまったため、チームで原因を分析し、対策を運用することにした。

9. 情報セキュリティ教育のまとめ

第9章 「情報セキュリティ教育のまとめ」

9. 情報セキュリティ教育のまとめ

情報セキュリティを意識しよう！

・ルールの理解・遵守に努める

・ルールに書いていない場合、情報セキュリティ維持のためにどうすべきか考えることが必要

・情報セキュリティ事故を起こさない、という意識を維持し続けることが大切

情報セキュリティ事件・事故に対して既にいろいろな教育や啓発に取り組んでいることと思います。

でも、情報セキュリティ事故件数はゼロになっていません。
むしろ、貸与品紛失、メールの誤送信など、基本的、初歩的な事故程多く発生しています。
あたりまえのルールが、いつのまにか守られていないのです。

最近普及してきた新しいビジネススタイルへ対応するためのルールも含め、それらルール遵守に努めることはもちろん、ルールに書いていないケースの質問については、各自で考えた上で情報セキュリティを維持するための判断が必要です。
その際に、不明点があれば、同僚や上長、また各社の情報セキュリティ担当部署へ相談することが大切です。

情報セキュリティ事故を起こさない、という根本的意識付けには決して変化はありません。

情報セキュリティ事故によるリスクや影響を認識することで、情報セキュリティ事故を起こさない、という意識を維持し続けてください。

2025
情報セキュリティ教育
春期版
END

TCS一HD
情報セキュリティ室

以上で、「2025年度春の情報セキュリティ教育」を終了します。
質問は、各社の情報セキュリティ担当部署までお願いします。

解答

設問1	設問2	設問3	設問4	設問5
3	1	1、2、3	2	2
設問6	設問7	設問8	設問9	設問10
3	3	3	2	3