TCSグループ
関係外秘

情報セキュリティ教育

2023年度　春期版

TCS GROUP

TCSホールディングス
情報セキュリティ委員会

ただ今より、TCSグループ『2023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

情報セキュリティの必要性と本質を理解

↓

プロフェッショナルとしての自覚

↓

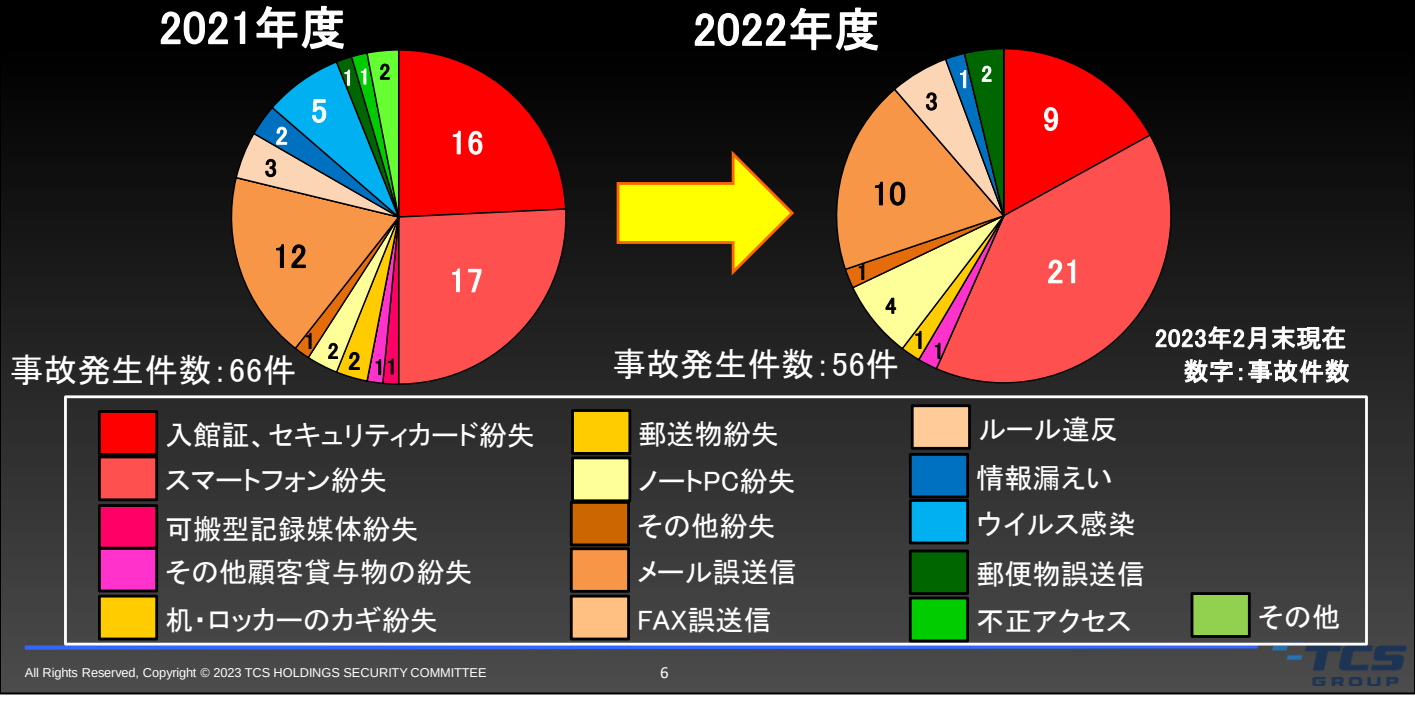
TCSグループの一員として適切な行動

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情報セキュリティ委員会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。

2022年度は全体の件数が前年度より減少傾向にありますが、スマートフォン、ノートPCなどの貸与物の紛失が増加しており、メールの誤送信は、前年度と変わらず多く発生しました。

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. 当社は、情報セキュリティポリシーとして、「機密情報管理規程」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01 情報セキュリティ基本方針」より

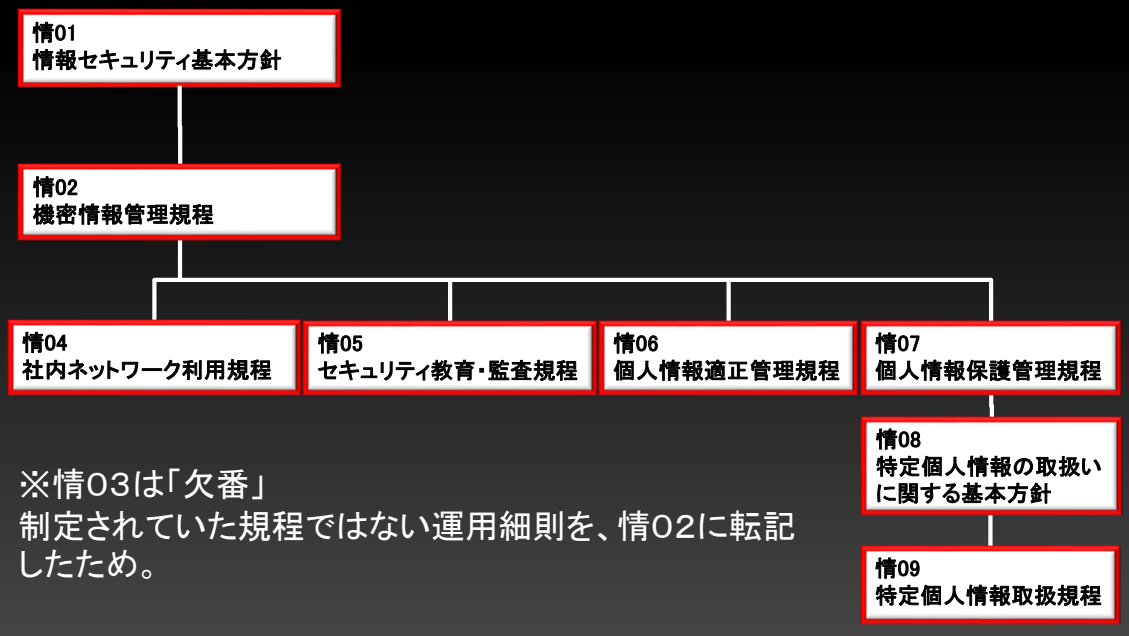
TCSグループは、情報セキュリティ基本方針を社内、社外に対し表明しています。

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. 当社は、情報セキュリティポリシーとして、「機密情報管理規程」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



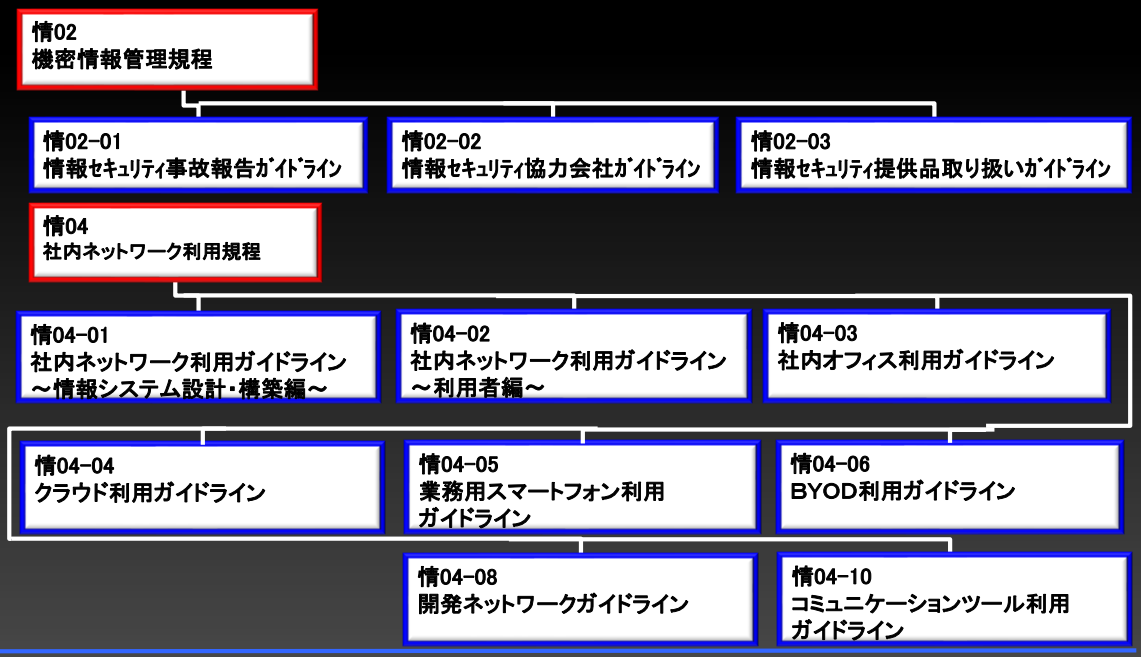
※情03は「欠番」
制定されていた規程ではない運用細則を、情02に転記したため。

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」、「個人情報保護管理規程」などが中心となります。

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、最近ではクラウド利用ガイドラインが2022年12月に改定されましたので、ご確認ください。

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
（情02） 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
（情04） 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
（情05） 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
（情06） 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
（情07） 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
（情09） 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TCS-ONEの「文書管理」に掲示
TCS-ONE文書管理：［全社員向け］>［セキュリティ］

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。

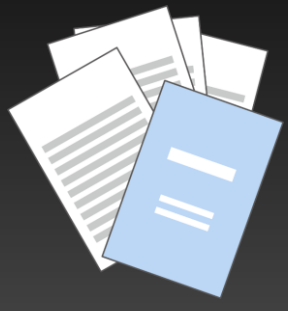
3. 物品の取扱い・業務中の行動について

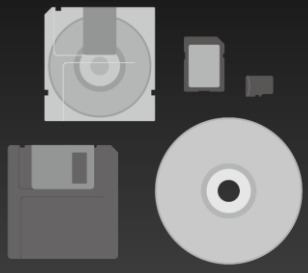
第3章 「物品の取扱い・業務中の行動について」

3. 物品の取扱い・業務中の行動について

貸与品の管理

- 貸与品は定期的に所在を確認する
- 必ず受領・返却の記録を残す





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。
具体的には入館証、社給のPCやスマホ、開発情報やデータなどです。

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。
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いましょう。

3. 物品の取扱い・業務中の行動について

貸与品管理の必要性

- 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

- **あなたの不注意がお客様先に重大な損害を与える可能性があります**
  - →損害賠償請求や信用失墜、取引停止など深刻な影響を与える危険性あり
- 不要になったら速やかに返却

定期的に注意喚起をしていますが、入館証やセキュリティカードの紛失があとを絶ちません。

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、他のものを取り出す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。
などが挙げられます。
そもそも、貸与品の入ったカバンを網棚に置くことは論外です。

もしも悪意を持った第三者が、あなたの紛失した入館証を使って顧客のオフィスに入り、機密情報を盗んで悪用したとしたら、あなたの不注意が原因で顧客先に重大な損害を与えてしまうかもしれないのです。
そうなれば、あなた個人に対して損害賠償が発生する可能性や会社が信用を失い、TCSグループ全体で取引停止になるかもしれないなど、影響は計り知れません。
貸与品をしっかり管理する、ということはとても大切なことです。

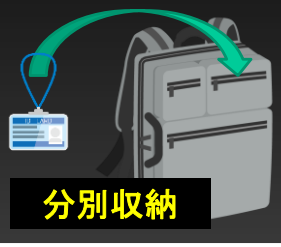
また、預かる期間が短ければ短いほど、紛失のリスクは減ります。
使う必要がなくなった情報や入館証等は、速やかに顧客に返却してください。
財布などに入館証やセキュリティカードを入れ不用意に持ち歩かない等、紛失リスクは最小限になるよう工夫しましょう。

3. 物品の取扱い・業務中の行動について

貸与品の紛失予防事例

入館証紛失の予防策

- 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



万全の注意を払い紛失を予防しよう！

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。

フォルダーだけチェックするのではなく、入館証が存在すること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・分別収納ができるものを選ぶなどの工夫をしましょう。

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ない、タスキ掛けにするなどして肌身離さず持つようにしましょう。

休日にビジネス用カバンを持ち歩いて紛失しないよう、ビジネス用と普段用は分けましょう。

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ダブルロックにするなどの対策を講じましょう。

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、定期的に所在は確認しましょう。

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、など工夫しましょう。

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。

上記ポイントで万全の注意を払い紛失を予防しましょう。

コピー・廃棄

- **記録媒体の廃棄**
  - データは完全に消去
  - 記録媒体は破壊する

記録媒体の破壊

ツールで消去

- **安全な業者にデータ消去を依頼**
  - データ消去証明書の中身を確認

データ消去証明書の詳細の確認

データ消去証明書

何を消去・破壊したのか確認

- **紙の廃棄**
  - シュレッダーか廃棄ボックス
  - 裏紙として使用しない

ディスク（HDD、SSD）やUSBメモリは、消去したつもりでも特殊なソフトウェアや装置を使ってデータを復元できます。
このような記録媒体から、情報が流出する事故も世間では発生しています。
破棄する際にはデータ削除は必須ですが、データを復元できなくするための専用の消去ツールを使ってください。
これによりデータを復元することが困難になり、情報流出を防ぐことができます。
CDやDVDを破壊する機能のあるシュレッダーもあります。
CDやDVDなどは破壊してから破棄してください。

またサーバやPCの廃棄を委託する場合も同様です。
データが復元できないことの証明となるデータ消去証明書が発行できる業者に委託し、発行された証明書の中身についても確認してください。

第三者に見られ情報が流出することを防ぐため、業務で使用した紙はシュレッダーに掛けるか、業者と契約した専用の廃棄ボックスに捨ててください。
また、裏紙として再利用はしないでください。

情報は増やさない、不用な情報は持たない、という大原則を、常に意識してください。

3. 物品の取扱い・業務中の行動について

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るの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。このようなことを行ってはなりません。

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ないよう注意してください。

画面は自動で切り替わります

残り [redacted]

設問1

入館証紛失の予防策において、不適切なものを選択しなさい。

1. 入館証は財布と一緒にカバンのポケットに入れて通勤している。

2. 入館証はカードフォルダーにいれている。カード所在とあわせて、フォルダーに破損がないかチェックしている。

3. 入館証は出勤前、また帰宅後に所在を確認している。

TCS GROUP

設問1　入館証紛失の予防策において、不適切なものを選択しなさい。

1. 入館証は財布と一緒にカバンのポケットに入れて通勤している。

2. 入館証はカードフォルダーにいれている。カード所在とあわせて、フォルダーに破損がないかチェックしている。

3. 入館証は出勤前、また帰宅後に所在を確認している。

画面は自動で切り替わります

残り [redacted]

設問2

公共の場所での行動について、適切なものを選択しなさい。

1. 客先へ電車で移動中、プレゼンの資料に目を通して過ごした。
2. 客先のエレベータ内で、業務についての雑談を交わした。
3. 喫煙所では、業務にかかわる会話はしない。

TCS GROUP

設問2　公共の場所での行動について、適切なものを選択しなさい。
1. 客先へ電車で移動中、プレゼンの資料に目を通して過ごした。
2. 客先のエレベータ内で、業務についての雑談を交わした。
3. 喫煙所では、業務にかかわる会話はしない。

4. デバイスの使用について

第4章 「デバイスの使用について」

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情報漏えい、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
  - 無料利用条件に該当せずライセンス違反

- **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

社給デバイスとは、会社が貸与した、業務で使用するパソコン、タブレット、スマホなどの総称です。
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
・ウイルス感染による機密情報の漏えいや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窃盗
・デバイスの紛失・盗難
・無償利用の条件に自社は該当しないのにインストールしてライセンス違反
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。
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**
  - PC管理専用ソフト導入、PC環境管理やライセンス管理に利用している
  - 社外からの各種アップデートが可能となった
  - 標準ウイルス対策ソフトがApexOneからDefenderへ

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。

社給デバイスをしっかり管理するために、PC管理専用ソフト(Skysea)を導入し、PC環境管理やライセンス管理に利用しています。

在宅勤務が常態化していることから、在宅勤務で利用しているPCに対し社外からもアップデートが行えるようになりました。

グループ標準のウイルス対策ソフトを、これまでのApexOneからマイクロソフト社のDefenderに変更しました。

ご自分が利用している環境をよく理解してしっかり管理してください。

社給スマホの利用拡大

- **紛失すると・・・**
  - 社給スマホ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。

近年社給スマホの紛失事故も増加しており、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。

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。

テレワークでの注意点

- **利用デバイスの注意点**
  - 社給デバイスで業務を行う。原則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、テレワーク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
  - PCにSkyseaを導入、確実に管理できる状態に

テレワークでの勤務は、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直接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。

テレワークの時には、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ましょう。

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ましょう。

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、テレワーク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。

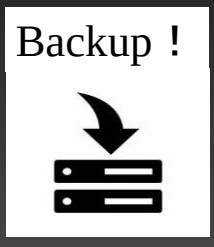
社給スマホを挟むことで、外部からの不正アクセスに対して社給スマホがファイアウォールとなり、社給PCを保護します。

現在のTCSグループでは、在宅勤務の方法として緊急対応的に導入したシンテレワークシステムですが、利用いただいている方は、会社設置PCとテレワークで使用するPCの双方にSkyseaを導入し、確実に管理できる状態にしてください。

コンピュータウイルス対策

- ウイルス対策ソフトを入れ、パターンファイルや定義ファイルを常に最新化すること

- ウイルス感染リスクを意識し、注意を払う
  - ソフトウェアには最新のセキュリティパッチを適用する。
  - 万が一のためにデータバックアップをしておく



ウイルスからPCを守る手段としてウイルス対策ソフトを入れ、パターンファイルや定義ファイルを常に最新化させてください。

ただし、ウイルス対策ソフトがあるから安心するのではなく、ソフトウェアには最新のセキュリティパッチを適用する、万が一のためにデータバックアップをしておくなど、普段からウイルス感染リスクを意識し、注意を払うことが大切です。

4. デバイスの使用について

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

対応のタイミング	対応内容
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
ウイルス検知が出来ない場合	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委員より TCS-HD情報セキュリティ委員会へ報・連・相
- 感染したコンピュータを再使用する場合は
  - ➢ コンピュータを初期化してネットワーク接続

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委員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。

・ウイルス対策ソフトの最新のパターンファイルを入手し、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委員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委員よりTCS－HD情報セキュリティ委員会へ報・連・相をしてください。

ウイルス感染したPCを再使用する場合は、PCの初期化インストールを行い、初期状態にしてから自社ネットワークに接続してください。

Wi-Fi利用時の注意

- **Wi-Fiの利用**
  - どこでも使えて便利だが、盗聴リスクが高い
    →悪意ある人が正規のアクセスポイントに
    なりすましている事がある
  - **Wi-Fiを使用する際の注意**
    ・適切に管理、運用されていないWi-Fi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
  - **個人で勝手にWi-Fiアクセスポイントを設置しない事！**
  - **社給デバイスでフリースポットに接続しない事！**

最近ではTCSグループが管理、運用しているWi-Fiが設置されている拠点が増えています。
Wi-Fiは物理的に見えないネットワークのため、セキュリティ対策を行わなければ悪意ある第三者に利用されるリスクが高くなります。
Wi-Fiアクセスポイントになりすました第三者にデータを盗まれたり、破壊されたりする可能性もあります。

適切に管理、運用されていないWi-Fiを設置し、使用することはルール違反となります。
Wi-Fiを設置する際は、社内ネットワーク利用ガイドライン～情報システム設計・構築編にしたがい、
構築、運用を行ってください。
なおPCだけでなく、社給スマホをフリースポットに接続する事は禁止です。
フリースポットの多くは通信の暗号化強度が十分でない、もしくは暗号化されていないことにより、データはほぼ丸裸で誰にでも見えてしまう可能性があります。
Wi-Fiに自動的に接続しない設定となっているか、もう一度確認しましょう。通常はWi-Fi通信設定自体をOFFにしておくのも良いでしょう。

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、不適切なものを選択しなさい。

1. ストラップをつけると邪魔なので社給スマホには何もつけていない。
2. 端末ロックは一定時間が過ぎると自動にロックがかかる設定にした。
3. 電話帳にある過去に参画したプロジェクトのお客様電話番号は不要となったら速やかに削除している。

TCS GROUP

設問3　社給スマホに関する文章のうち、不適切なものを選択しなさい。

1. ストラップをつけると邪魔なので社給スマホには何もつけていない。
2. 端末ロックは一定時間が過ぎると自動にロックがかかる設定にした。
3. 電話帳にある過去に参画したプロジェクトのお客様電話番号は不要となったら速やかに削除している。

画面は自動で切り替わります

残り [redacted]

設問4

テレワークに関する文章のうち、適切なものを選択しなさい。

1. テレワークで使用している社給PCの調子が悪いので、許可を取っていない私用PCを緊急措置として使用した。
2. テレワークで使用している社給PCのOS、ウイルス対策ソフトの更新は定期的に行っている。
3. ネットワークの通信状況が悪かったため、自宅のネットワークに直接社給PCを接続した。

TCS GROUP

設問4　テレワークに関する文章のうち、適切なものを選択しなさい。

1.テレワークで使用している社給PCの調子が悪いので、許可を取っていない私用PCを緊急措置として使用した。

2.テレワークで使用している社給PCのOS、ウイルス対策ソフトの更新は定期的に行っている。

3.ネットワークの通信状況が悪かったため、自宅のネットワークに直接社給PCを接続した。

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. PCを使用中に怪しげな画面が表示され、ウイルスに感染したと思い、直ちにインターネットから切断した。

2. PCでの業務中、ウイルス感染メッセージが表示された。すぐに、ウイルス駆除を実施し、すべての作業が完了後、上司に報告した。

3. ウイルス対策ソフトをインストールし、パターンファイルは常に最新化している。

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. PCを使用中に怪しげな画面が表示され、ウイルスに感染したと思い、直ちにインターネットから切断した。

2. PCでの業務中、ウイルス感染メッセージが表示された。すぐに、ウイルス駆除を実施し、すべての作業が完了後、上司に報告した。

3. ウイルス対策ソフトをインストールし、パターンファイルは常に最新化している。

5. ビジネスツール使用について

第5章 「ビジネスツール使用について」

5. ビジネスツール使用について

メール利用の注意事項

- **メールからコンピュータウイルスに感染する原因**
  - 見知らぬアドレスからのメールを安易に開く
  - プレビュー機能を有効にしていた
  - 添付ファイルを信用しダウンロードした
  - メールに記載のURLリンクにアクセスした

- **対策**
  - 見知らぬアドレスからのメールは安易に開かない
  - プレビュー機能を無効にする
  - 添付ファイルを安易にダウンロードしない
  - URLリンクに安易にアクセスしない
  - OSやソフトウェアのアップデートはすぐ行う

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、メールからコンピュータ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。
メールからコンピュータウイルスに感染する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送信され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。
・添付ファイルを信用しダウンロードした。
・メール本文に記載されているURLリンクにアクセスした。

対策として、
・見知らぬ相手からのメールは安易に開かず信頼できるアドレスから送られてきているか確認する。
・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リンクに安易にアクセスせず、信頼できるURLか確認する。
・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. ビジネスツール使用について

メール利用の注意事項

- **メール誤送信及び情報漏えいの原因**
  - 送信前の宛先確認不足
  - 安易な全員返信
  - オートコンプリート機能による宛先誤り
  - 添付ファイルの誤り
- **対策**
  - メール送信前は必ず宛先を確認する
  - 安易な全員返信をしないでBCCを活用する
  - オートコンプリート機能は無効にする
  - 安易にファイル添付しない
  - ファイル添付をしたら、送信前にファイルを開いて添付誤りでないか確認する

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。

メール誤送信のケースとして以下の原因が挙げられます。
・送信前の宛先確認不十分。
・初めてメールする相手のメールアドレス確認不足。
・安易な全員返信。
・宛先候補を表示するオートコンプリート機能により、誤った宛先を選択。
・添付ファイルの誤り。

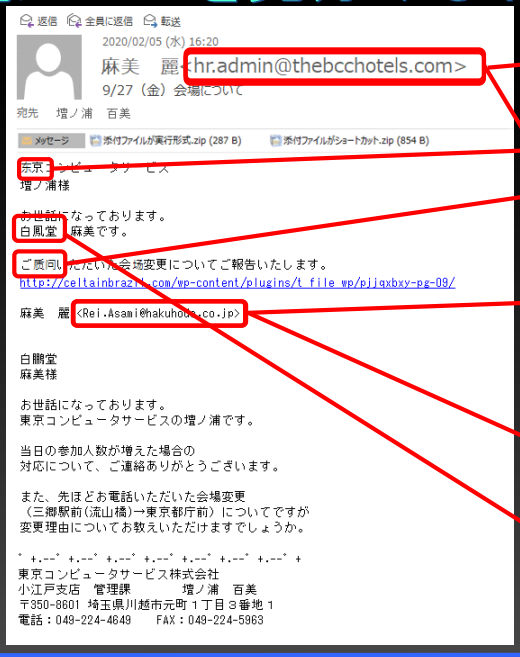
対策として、
・メール送信をする前に必ず送信相手のメールアドレス、名前、会社名、添付ファイルの内容を確認してください。
　確認するための方法として以下が挙げられます。
・メールソフトの誤送信対策機能である自己承認機能を活用し、氏名、アドレス、添付ファイルの再確認を行ってから送信する。
・初めてメールする相手には、名刺に記載されているメールアドレスを確認してから送信する。又は、直接本人に電話してメールアドレスの確認をしてから送信する。
・同姓の宛先設定誤りを防ぐため、アドレス帳の登録名を区別できるよう氏名の前に会社名を付けるなど適宜見直しを行う。
・一斉送信や全員返信の場合、メール設定で警告を表示するようにし、送信相手に他者のメールアドレスが参照されないよう
　BCCに宛先を変更する。
・オートコンプリート機能は便利な反面、同姓によるミスを起こしやすいため無効にする。
・情報漏えいの低減のため、安易にファイル添付をしない。
・ファイル添付をするときは、送信前に、必ず添付ファイルをもう一度開いてファイルが正しいか確認する。
　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貼り、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。

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。
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。

メールの送信は慎重におこないましょう。

5. ビジネスツール使用について

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@thebcchotels.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

お世話になっております。
東京コンピュータサービスの壇ノ浦です。

当日の参加人数が増えた場合の
対応について、ご連絡ありがとうございます。

また、先ほどお電話いただいた会場変更
（三郷駅前(流山橋)→東京都庁前）についてですが
変更理由についてお教えいただけますでしょうか。

東京コンピュータサービス株式会社
小江戸支店　管理課　　壇ノ浦　百美
〒350-8601 埼玉県川越市元町１丁目３番地１
電話：049-224-4649　　FAX：049-224-5963

送信元アドレスの@マーク以降がフリーメールアドレス等
例）xxxxxxxx@example.com

日本語で使用されない漢字、不自然な日本語
例）東京⇒东京、質問⇒质问

表示アドレスが公表されているアドレスと異なる
例）正：amazon
　　誤：amazone

送信元アドレスと署名が不一致
例）xxxxxxxx@example.com
　　xxxxxxxx@example.co.jp

送信元の組織名、電話番号が実在しない

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ましょう。

【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)

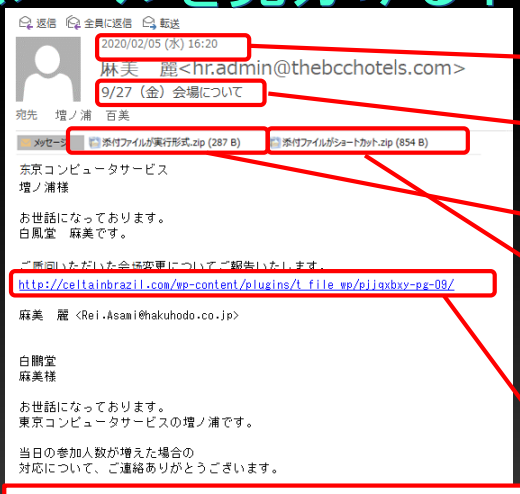
送信元の組織名や電話番号をメール以外の情報源から調べても実在しない。

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. ビジネスツール使用について

迷惑メールを見分けるポイント



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（添付ファイルを開封するとexeファイル等の実行形式ファイル）

添付ファイルがショートカットファイル（添付ファイルを開封すると、ショートカットファイルとなっている）

URLが不一致
例）
表示：http://celtainbrazil.com/wp-content/plugins/t_file_wp/pjjqxbxy-pg-09/
参照先URL：　http://celtainbrazil.co.XX/wp-content/plugins/t_file_wp/pjjqxbxy-pg-09/

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。

最近、TCSグループ社員を騙った迷惑メールも増加しています。

不審なメールには十分注意し、メール及び添付ファイルを安易に開かないようにしましょう。

5. ビジネスツール使用について

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。

＜ご参考：フィッシングメール注意喚起＞

●厚生労働省
新型コロナウイルスを題材とした攻撃メールについて

●Amazon
AmazonからのEメール、電話、テキストメッセージ、またはウェブページかどうかを見分ける

●ヤマト運輸
ヤマト運輸の名前を装った「迷惑メール」および「なりすましサイト」にご注意ください

●楽天市場
【ご注意ください】楽天を偽装したサイト・メール等

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。

参考までに、フィッシングメールの対応について、サイト上で各社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。

■この欄、ここから下は読みません。

※＜ご参考：各社のフィッシングメール注意喚起＞

●厚生労働省

https://www.mhlw.go.jp/stf/newpage_09393.html

●amazon

https://www.amazon.co.jp/gp/help/customer/display.html/ref=hp_left_v4_sib?ie=UTF8&nodeId=G4YFYCCNUSENA23B

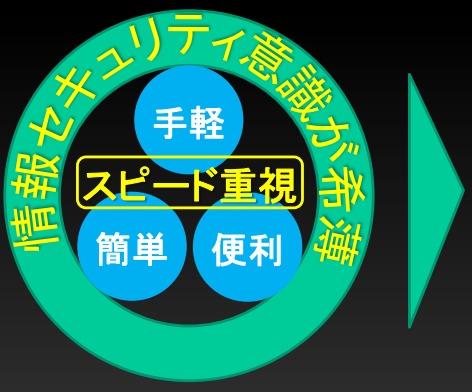
●楽天市場

https://corp.rakuten.co.jp/security/anti-fraud/

●ヤマト運輸

https://www.yamato-hd.co.jp/important/info_181212.html

チャットツール



何気なく・・・・
機密情報を書き込む
個人情報を含むデータを送付する
URLをクリックする
添付ファイルを開く

簡単に情報セキュリティ事故が発生するリスクがある
改めてコミュニケーションツール利用ガイドラインを確認する

チャットツールはここ数年で一気に普及が進みました。
コミュニケーションの円滑化や業務効率化などメリットが多い一方で、情報漏えいなどセキュリティリスクが存在することにも注意を払いましょう。

チャットツールでは手軽にコミュニケーションが取れ、情報共有がスムーズにできます。
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、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、
・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。
・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。
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。

今後ますますチャットツールの利用が広がっていくことからも、改めてコミュニケーションツール利用ガイドラインを確認しておきましょう。

5. ビジネスツール使用について

Web会議の使い方

- Web会議での注意
  - 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
- Web会議を主催する場合の注意
  - 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、強制退去など
- ゲストとして招待される場合の注意
  - 招待されたURL/会議室番号等が信頼できる所か確認する

新卒採用でWeb会議を主催する場合、あるいはインターネット上で行われるセミナー参加やお客様との会議等でWeb会議を使用する場合、以下のことに注意してください。

- 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会議を主催者として開催する場合、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、使いまわしはやめましょう。

さらに、会議参加者の出席確認を実施してください。

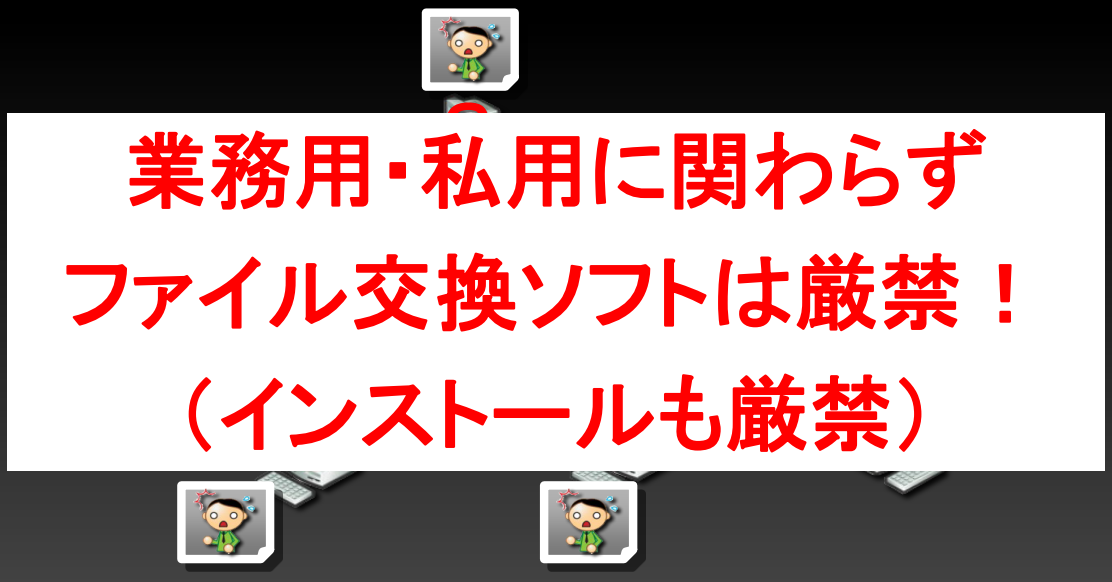
会議には招待した特定の人以外は、参加できないように対策することも重要です。

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所か確認してください。

ファイル交換ソフト



ファイル交換ソフトは情報漏えいに繋がるソフトとして、TCSグループでは会社でも自宅でも、使用を禁止しています。

このファイル交換ソフトとは、インターネットに接続した不特定多数の利用者間で、ファイルを交換し合うためのソフトウェアです。

ファイル交換ソフトをインストールした端末は、「スパムメールの送信」や「DDoS攻撃」の踏み台となるようなウイルスに感染するリスクが高くなります。

ウイルス感染の結果、公開するつもりの無いファイルまで公開されてしまいます。

一度公開されてしまったファイルを回収することは不可能であり、さらなる情報拡散につながることもあります。

ファイル交換ソフトは決してインストールしないでください。

画面は自動で切り替わります

残り [redacted]

設問6

メール利用に伴うウイルス感染予防について、適切なものを選択しなさい。

1. 不審なメールをいち早く確認するため、メールプレビュー機能を有効にしている。
2. 知らない担当者からのメールを受信したが、いつもの取引先と同じ会社名だったため、メールを開いて内容を確認した。
3. 突然取引先より、“至急添付ファイルを確認ください”とのメールを受信した。急いでいるようであったが、初めてメールをいただいたお客様であったため、いきなり添付ファイルをダウンロードせず、直接電話でお客様に要件を確認した。

設問6　メール利用に伴うウイルス感染予防について、適切なものを選択しなさい。

1. 不審なメールをいち早く確認するため、メールプレビュー機能を有効にしている。

2. 知らない担当者からのメールを受信したが、いつもの取引先と同じ会社名だったため、メールを開いて内容を確認した。

3. 突然取引先より、“至急添付ファイルを確認ください”とのメールを受信した。急いでいるようであったが、初めてメールをいただいたお客様であったため、いきなり添付ファイルをダウンロードせず、直接電話でお客様に要件を確認した。

画面は自動で切り替わります

残り [redacted]

設問7

メール誤送信防止の対応として、不適切なものを選択しなさい。

1. 誤送信を防ぐため、メールの誤送信防止対策機能を有効にし、送信前に必ず宛先を確認している。
2. 誤送信を防ぐため、オートコンプリート機能を有効にし、同姓同名のアドレスで誤りがないか確認してからメール送信している。
3. 初めてメール送信する相手には、あらかじめメールアドレスを確認してからメール送信している。

設問7　メール誤送信防止の対応として、不適切なものを選択しなさい。

1. 誤送信を防ぐため、メールの誤送信防止対策機能を有効にし、送信前に必ず宛先を確認している。
2. 誤送信を防ぐため、オートコンプリート機能を有効にし、同姓同名のアドレスで誤りがないか確認してからメール送信している。
3. 初めてメール送信する相手には、あらかじめメールアドレスを確認してからメール送信している。

画面は自動で切り替わります

残り [redacted]

設問8

Web会議の使用について、不適切なものを選択しなさい。

1. お客様からWebセミナーへの出席要請があったので、URLを確認せずアクセスした。
2. 開催したWeb会議の録画ファイルは自分のPCに格納後、自社ファイルサーバーに保管した。
3. 電車で移動中、Web会議への参加を要請された。情報漏えい防止のため、社内に戻ってからWeb会議に参加した。

TCS GROUP

設問8　Web会議の使用について、不適切なものを選択しなさい。

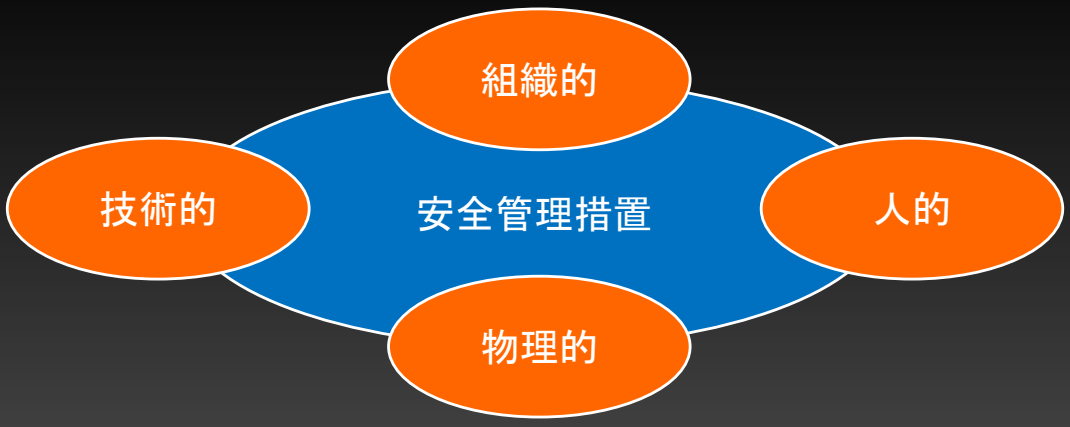
1. お客様からWebセミナーへの出席要請があったので、URLを確認せずアクセスした。
2. 開催したWeb会議の録画ファイルは自分のPCに格納後、自社ファイルサーバーに保管した。
3. 電車で移動中、Web会議への参加を要請された。情報漏えい防止のため、社内に戻ってからWeb会議に参加した。

6. 個人情報保護について

第6章 「個人情報保護について」

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



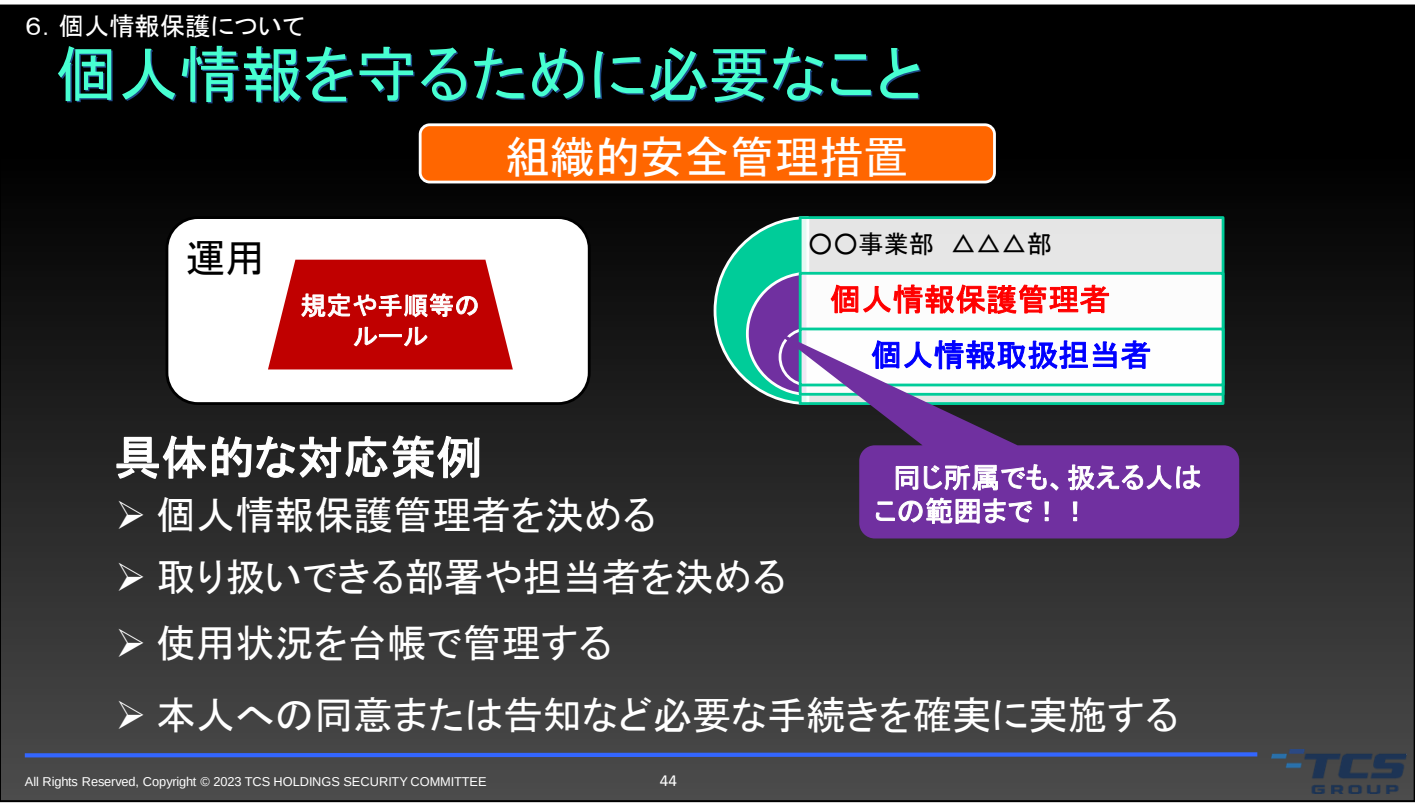
個人情報保護のために、個人情報を扱う場合、「安全管理措置」を実施することが個人情報保護法で義務付けられています。

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

誓約書・同意書等を締結します

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締結しています。

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。

また、社員の皆さんに対して、会社が収集した皆さんの個人情報の利用目的と開示範囲を明確にするために、同意書を締結しています。

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。

近年の改正ポイント

仮名加工情報・・・他の情報と照合すれば個人を特定できるように
加工された情報
匿名加工情報・・・特定の個人を識別できないように加工し
復元できないようにした情報
（個人識別符号は削除しなければならない）
個人識別符号・・・個人を識別できる文字や記号といった符号のこと
個人関連情報・・・生存する個人に関する情報であって、個人情報、
仮名加工情報、匿名加工情報以外のもの

個人情報の取得や利用についての規制が強化された
・不適切な利用禁止
・利用目的の特定と通知

近年の改正ポイントとして以下の概念が導入されており、よく似た名称のため取り違えないように扱う個人情報がどのようなものかしっかり理解しましょう。

仮名加工情報は他の情報と照合すれば個人を特定できるように加工された情報
匿名加工情報は特定の個人を識別できないように加工し復元できないようにした情報
（なお、個人識別符号は削除しなければいけません。）
個人識別符号は個人を識別できる文字や記号といった符号のこと。
個人関連情報は生存する個人に関する情報であって、個人情報、仮名加工情報、匿名加工情報以外のものです。

また個人情報の取得や利用についての規制が強化されており、個人情報を取り扱う際は
不適切な利用禁止
利用目的の特定と通知
といった点も十分に理解した上で実務にあたる必要があります。

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誤っている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. 会社は社会保障及び税に関する手続書類の作成事務をするために、マイナンバーが必要である。

設問9　マイナンバー制度に関して誤っている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. 会社は社会保障及び税に関する手続き書類の作成事務をするために、マイナンバーが必要である。

7. 事故発生時の対応

第7章 「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。

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情報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。

7. 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グループの方の電話番号やメールアドレス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。

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。

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。

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の発生時の対応として、適切なものを選択しなさい。

1. 出勤時に社給スマホを紛失している事に気が付いた。どこで紛失したか心当たりがないため、出勤途中、急いで最寄りの交番で遺失物届を行ってから出社した。
2. 取引先に誤って他社の顧客情報をメール送信してしまった。誤送信先にメールの削除を電話で依頼した。削除対応してもらえたので、対応完了後、上司に詳細を報告した。
3. 帰宅後、顧客先の入館証がカバンに入っていない事に気が付いた。就業先に置き忘れたかもしれないと思ったが、すぐに上司に第一報を行って、指示を仰いだ。

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

1. 出勤時に社給スマホを紛失している事に気が付いた。どこで紛失したか心当たりがないため、出勤途中、急いで最寄りの交番で遺失物届を行ってから出社した。

2. 取引先に誤って他社の顧客情報をメール送信してしまった。誤送信先にメールの削除を電話で依頼した。削除対応してもらえたので、対応完了後、上司に詳細を報告した。

3. 帰宅後、顧客先の入館証がカバンに入っていない事に気が付いた。就業先に置き忘れたかもしれないと思ったが、すぐに上司に第一報を行って、指示を仰いだ。

8. 情報セキュリティ教育のまとめ

第8章 「情報セキュリティ教育のまとめ」

8. 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委員に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。

以上で、「2023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委員会までお願いします。

解答

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