CTC
Challenging Tomorrow's Changes

弊社のセキュリティに関する取り組みと実例

伊藤忠テクノソリューションズ株式会社

【本日お話しする事】
1. 弊社の紹介、人事部の紹介、自己紹介
2. 弊社のセキュリティに関する取り組み
3. CTC社員のセキュアーな一日
4. ビジネスマンに求められるセキュリティ感性

弊社の紹介、人事部の紹介、自己紹介

会社紹介

会社名:	伊藤忠テクノソリューションズ株式会社(略称CTC)
本社所在地:	〒100-6080　東京都千代田区霞が関3-2-5　霞が関ビル
創立:	1972年4月1日
社員数:	4,029名（CTCグループ：8,303名 2016年4月1日現在）
代表取締役社長:	菊地　哲
事業内容:	コンピュータ・ネットワークシステムの販売・保守、ソフトウェア受託開発、 情報処理サービス、科学・工学系情報サービス、サポート、その他

人事部 紹介

組織:　経営管理グループ　人事総務室　人事部

人事統括課、人事企画課、労務課、キャリア課、ダイバーシティ推進課、健康支援室、人材開発課

自己紹介

略歴:	入社1982年	金融機関のATM開発に従事
		株式管理システムの再構築に従事
	転職1994年	経理システム、外為システムの再構築に従事
	異動2005年	ﾌﾟﾛｼﾞｪｸﾄﾏﾈｼﾞﾒﾝﾄ教育に携わる

CTCグループでは、ISO27001およびプライバシーマークに準拠し、情報セキュリティマネジメントシステムと個人情報保護マネジメントシステムとを統合した「情報セキュリティ・個人情報保護マネジメントシステム」（以下「ISMS」）を構築し、運用しております。

弊社のセキュリティに関する取り組み

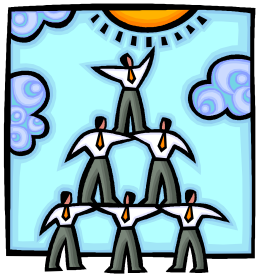
◆組織体制について

1）CTCグループ全体のISMSを統括する責任者としてチーフコンプライアンスオフィサー(CCO)を**「情報セキュリティ担当役員」**に任命

2）部署・サイト単位で**「情報管理責任者」**（部署長）を置くと共に、ISMSを推進する担当者として**「情報管理リーダ」**を任命

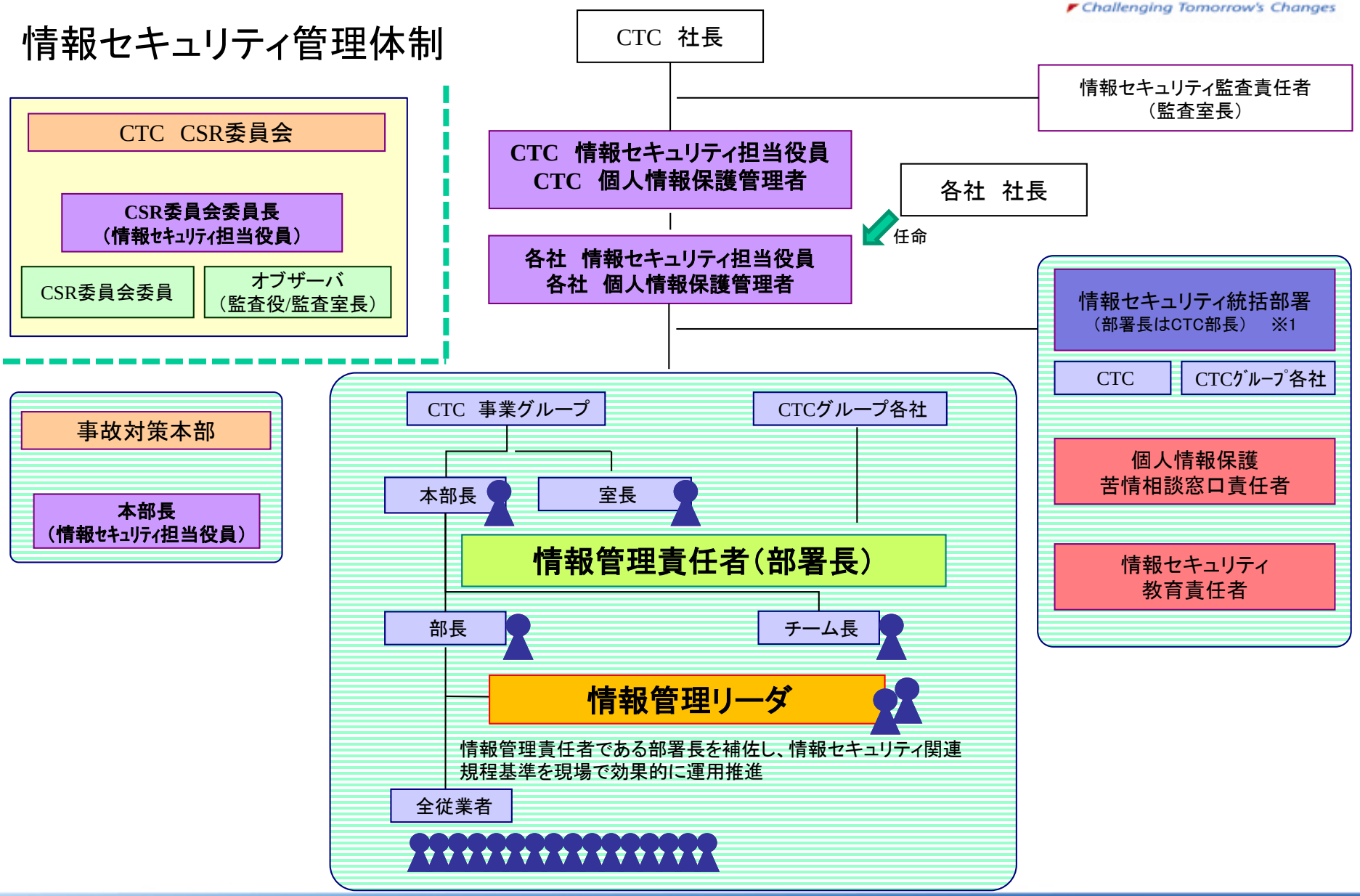
3）情報セキュリティを主管とする専任部署として**「セキュリティ・工事監理部」**を設置

4）個人情報保護に関する**苦情・相談受付窓口**を常設
（セキュリティ・工事監理部が担当）



CTCグループのISMS体制（ご参考）

情報セキュリティ管理体制



◆教育・啓発活動について

1）情報管理リーダを対象とした、情報セキュリティ・個人情報保護
および情報セキュリティリスクアセスメントの集合教育（毎年）

2）グループ全役員・従業者を対象とした、eラーニングによる、
情報セキュリティ・個人情報保護教育（毎年）

3）役員研修、部長研修、課長・GL研修、入社時の職種別・職位別研修、
新任役職者研修において、情報セキュリティ・個人情報保護に
関して研修

4）社内イントラネット及び事務所内掲示板にCTCグループ行動基準、
CTCグループ情報セキュリティ基本方針、個人情報保護方針等を掲示

5）全社にメールによる通達、社内報での情報セキュリティ
記事掲載、毎朝の館内放送等による注意喚起

◆外部委託先に関する取り組みについて

1）基本契約締結に先立ち、委託先選定申請書およびチェックシートに基づく評価を実施

2）委託業務内容に応じて「情報セキュリティについての覚書」などセキュリティに特化した契約を別途締結

3）情報セキュリティおよび個人情報保護に関する調査を毎年実施

Challenging Tomorrow's Changes

◆PC等のセキュリティ管理について

1）PCのウイルス対策徹底とOSのセキュリティパッチ適用
原則自動更新、特に重要・緊急な場合には随時アナウンスし
適用を確認

2）システムによるPCからUSBポート経由での外部媒体への書き込み制限

3）全PCに暗号化ツールを導入済み（一部機能検証用等を除く）

4）PCおよび重要情報の社外持出規制
PCは原則社外持出禁止。お客さまからの要請に基づく場合のみ、
持ち出しを許可された専用のPCで必要条件をクリアしたうえで
持ち出し許可。情報の保管が可能なPCの持ち出しについては
都度使用履歴を台帳管理。

5）年1回のPC棚卸に実機確認

◆業務に係るシステム環境について

1）ID／パスワードによるアクセス管理、IDによるアクセス制御

2）データセンターを利用した業務用サーバの集中運用管理

3）Webサーバのセキュリティホールの常時監視

4）脆弱性診断結果に基づく改修

5）シンクライアント(記憶装置を持たない端末)の導入

6）携帯端末、スマートフォン、タブレット端末からの
　モバイル接続にあたって、セキュリティツールを導入

◆インターネットアクセス・メールの利用制限について

1）ネットワーク機器によるアクセス制限

2）メールやWebアクセスのログ取得・追跡

3）フィルタリングシステムによるインターネットアクセス制限および
　個人メールアドレスへの送信・転送制限

4）業務用途外のソフトウェアのダウンロードおよび使用禁止

5）社内PCからモバイルルータ経由での社外接続を遮断

CTC
Challenging Tomorrow's Changes

◆データの授受及び保管等の管理方法について

1）お客様からのお預かり情報の取り扱い・管理
①お客様からお預かりしている情報は、全て機密情報として、
受渡し確認、アクセス管理（施錠されたキャビネットへの保管、
アクセス制限をかけたディスクへの保管、ディスクの暗号化等）を実施
②「文書管理規程」により、保管方法／閲覧／複写制限／保存期限を
定めて管理

2）セミナー案内等で取得する個人情報はご本人の事前承諾を取得のうえ、
個人情報保護関連基準（JIS Q 15001準拠）に基づき、専用システムにより
一元管理

◆重要情報・情報機器の廃棄時の対策について

1）PC等の機器廃棄・返却時はデータ削除を徹底

2）お客さま情報は原則として返却。お客様から廃棄を
依頼された場合は管理者による確認を徹底。

◆その他、情報セキュリティ上の制限事項

1）USBメモリーは、お客様の特別な指示による場合等を除き使用禁止

2）Winnyなどのファイル交換ソフトやSoftEtherなどの
ソフトウェアVPNの使用禁止

3）私物のPC（事前に許可を得たものを除く）、私物の外部記憶メディアの
会社での使用禁止

4）Winnyなどのファイル交換ソフトを導入したことがある
自宅・私有PCでの会社情報の取り扱い禁止

◆入退管理・手続きについて

【従業員】
- 入館用カードによる入退管理
- 重要な設備については生体認証装置による入退管理

【来訪者】
- 受付にて社名、氏名を伺い、ゲストバッジを交付し、社員がアテンド
- 外来者の執務室入室は原則禁止

◆外部人材管理について

1）派遣元、業務委託先との機密保持契約の締結

2）本人からの誓約書（自社宛に提出した誓約書のコピー）取得

3）契約満了時のアカウント削除の徹底

弊社の社員がどれぐらいセキュリティを意識して、日々の業務に当たっているかを、1日の行動から見てみましょう

CTC社員のセキュアーな一日

出社から始業まで

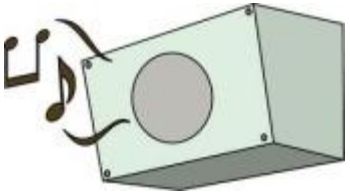
1日の始まりは社内のセキュアーな環境へ入室する事から始まります。
ICカードや生体認証でガードされた執務室エリアへは、社員以外は容易に入れません。
また、セキュリティに関する注意喚起も毎朝行われます。

社員証（ICカード）で第1扉を開く

生体認証（指紋、静脈）で第2扉を開く

社員番号と3か月おきに変更を求められるパスワードでPCにログイン

8:55にセキュリティ向上の声掛けが流れる



業務1（メール）

メールはもっとも間違いが起きやすくセキュリティ上とても気を使います。
ウイルスメールや人的ミスの発生をシステムでガードすることは当然ながら、人的な側面からも防いでいます。

人的にガード

重要な内容や
宛先の場合は
2人でダブルチェック
を行う事も

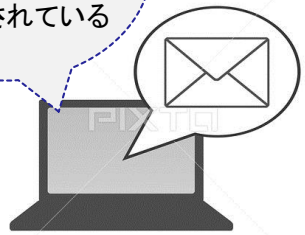
宛先が間違って
いないか？
添付ファイルを
間違っていないか？
PCに向かって
指さし確認！

そのパスワードも
そろそろ変更する
時期が来ている

パスワードは
事前に取り決めたもの
を利用する。

システムでガード

今朝もウィルスメールが
いくつか届いているが、
監視ソフトにより
無効化されている



社内の問い合わせ
に返信する。
送信ボタンを押すが
すぐには送信されない。
宛先と添付ファイルに
間違いがないか
確認の画面が出る

確認後送信ボタンを押しても
直ぐには送信されない。
送信されるまで
10秒間の合間があり、
送信を確認する
ことができる。

社外への添付ファイルは
パスワードを掛けないと
送信エラーになる

業務2（書類の閲覧、作成、破棄）

書類は、機密性/完全性/可用性に応じて管理レベルを設定し、廃棄についてのルールも設定しています。

キャビネから書類を出して確認する

キャビネの鍵を借りる ⇒ キャビネから書類を取り出し ⇒ 鍵を返却

新しい書類を作成する

作成した書類を管理台帳に記入

セキュリティレベルに応じて管理レベルを設定（保有期間、保管状況など）

年度が替われば書類もバインダーも新しくする

不要な資料は書類専用廃棄BOXに投入

シュレッダーと同等、投入後は取り出せない

管理期限が過ぎた書類を破棄する

管理台帳に記載された保有期限を過ぎた資料は定期的に破棄する

個人の荷物

袖机の利用制限、頻繁に使用する書類に限って収納

個人の荷物は個人ロッカーへ

外出

得意先や異なるオフィスへの情報の持ち出しは必ず発生します。
その際も決められたルールを遵守し、重ねて個人での注意をします。

社外への書類の持ち出し

お客様先に機密情報が含まれた書類を持ち出すためには部長の承認が必要。
社内の他オフィスではシンクライアントを利用し、極力書類を持ちださない。
どうしても持ち出す場合は、セキュリティ便の利用、二人で行動

社外でのPCの利用

持ち出し禁止PC

社外には一切持ち出せない

持ち出し専用PC

必要な情報のみ格納し、利用後に削除する
自宅/出張先には持っていけない

記憶装置を持たないPC

インターネットにつなげば、会社と同じ環境で仕事ができる
自宅/出張先にも持っていける

退社

勤務時間も終わり退社する時も、セキュリティの事をしっかり考えます。

後片付け

使った資料を所定キャビネットに戻し施錠する

よく利用する資料は袖机にしまい、施錠する

整理整頓

机の周りを整理整頓、不要な書類や書籍、文房具はおかない

個人の持ち物は個人ロッカーへ

アフター5

退社後もセキュリティの意識は高く保ちます。
電車に乗るとき、飲み会の席などでは特に注意します。

退社後に注意する事

- 書類は持ち帰らない
- 社外でみだりに会社の重要な話はしない
- 社員証や名刺などはカバンの特定の場所に収めみだりに取り出したりしない
- 網棚に鞄を置かない
- 緊急性がない要件で、社外から会社のシステムにはアクセスしない

セキュリティ事故を起こしたら

- それでもセキュリティ事故を起こしたら関係各所に連絡する

ビジネスマンに求められるセキュリティ感性

まとめ

ICTリテラシーとしてのセキュリティ

CTC
Challenging Tomorrow's Changes

システムですべてを守ることはできない。
個人と組織の意識を保ち続けることが重要。

情報漏えいは企業価値の失墜に直接つながる

昨今、ニュース・記事の枚挙にいとまがない

ルールやシステムで強固に守ることは基本、加えて重要な点は

- ルールを知ること、
  - 教育、不断の啓蒙
- ルールを守ること
  - 個人での注意、仲間との注意、組織での注意
- ルールが守られているか確認すること
  - 相互チェック
- セキュリティ事故を起こしたら委細関わらず報告すること