弊社のテレワーク取り組み及び
テレワーク導入の際の留意点について

2004年10月8日

NTTコミュニケーションズ株式会社

アジェンダ

1．テレワーカに求められるセキュリティ・リテラシーとは？
　（参考）CAVAスタッフによるテレワーク

2．トータルセキュリティを推進する三位一体の考え方

3．テレワーク環境におけるセキュリティリスクと対策

4．NTTコミュニケーションズにおけるテレワークの取組み
　4－1．eワーク（在宅勤務）のコンセプトと導入ステップ
　4－2．eワークの運用イメージ

1. テレワーカに求められるセキュリティ・リテラシーとは

1. お客様情報の保護について

お客様情報の定義・利用範囲の制限・委託管理に関わる対応 等

2. 業務上の情報の保護について

情報資産の定義・利用範囲の制限　等

3. ネットワークセキュリティの確保について

(不正アクセス、ウィルス等)

必要な対策・対策の実装の確認　等

4. 端末の管理について

(他人による物理的アクセス、破損、情報の持ち出し等)

必要な対策・対策の実装の確認　等

5. 業務従事者の意識の向上について

・セキュリティの重要性の認識

法的責任
契約上の責任
個人情報保護法による規定・契約による制限　等

・セキュリティ向上ための方策の理解

各セキュリティ施策に関しての理解　等

6. セキュリティ意識の向上施策

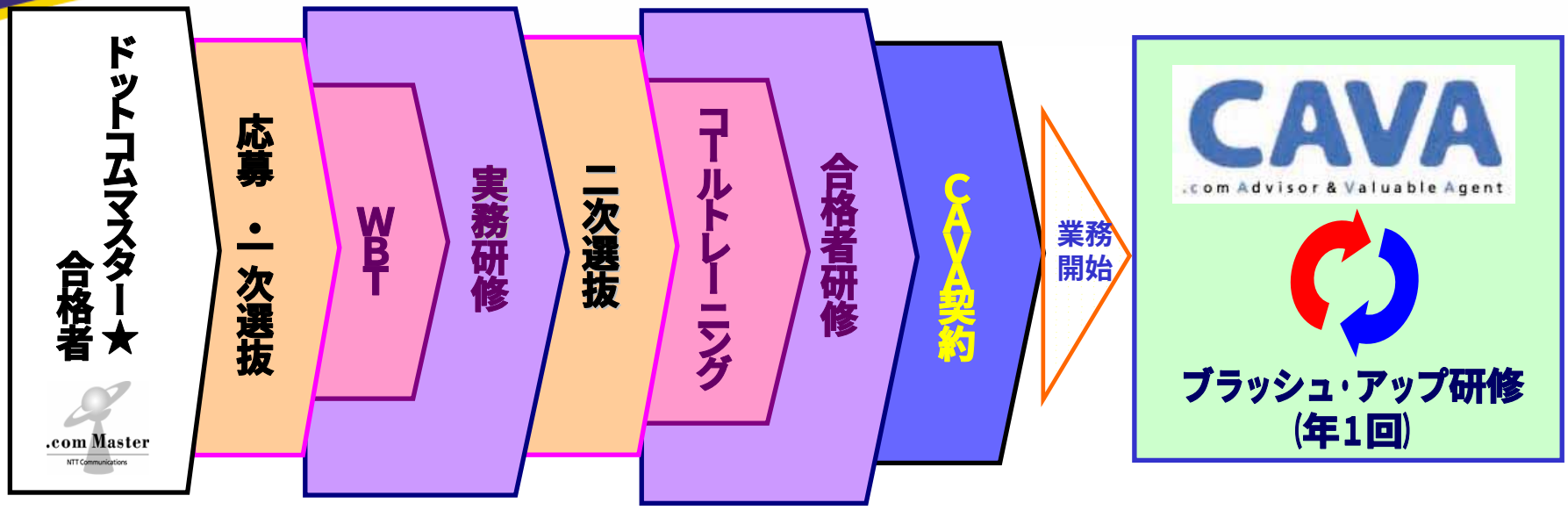
・業務従事前研修の実施

1～5の背景、考え方の理解・実装の方法

・継続的なブラッシュアップ
（WBTをベース。1年に一回程度の集合研修の実施など）

継続的な意識喚起の必要性・従事者全員の受講

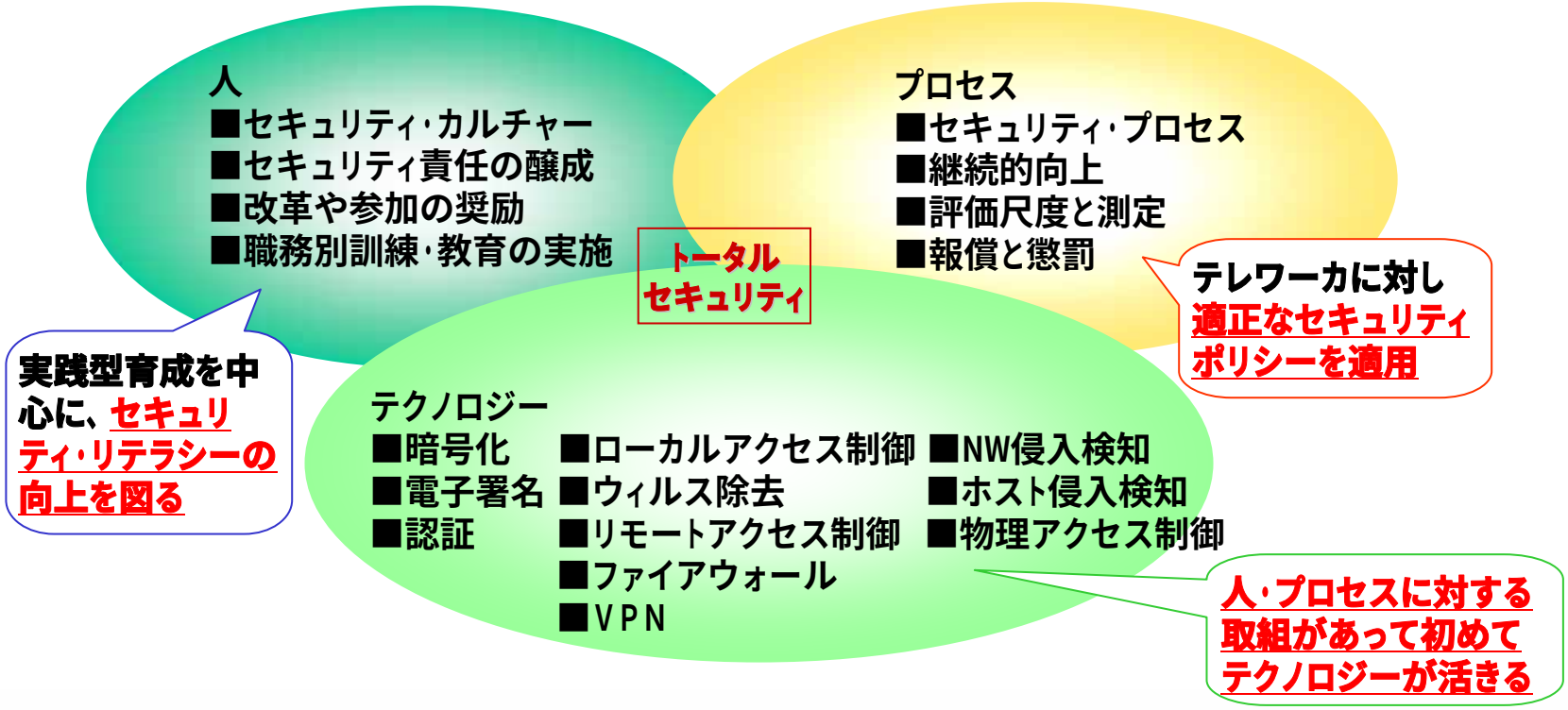
【参考】CAVAスタッフ（OCNサポート在宅オペレータ）によるテレワーク



ITスキル担保	応対スキルの向上・CSの担保		セキュリティの担保・契約の理解	スキル維持・セキュリティの向上
「.com Master★」カリキュラム 1. ハードウェアとOS 2. アプリケーション設定と使いこなし 3. インターネットの技術 4. サービス提供 5. 利用に関する知識	WBTカリキュラム ・OCN業務知識 ・OCN商品知識 ・OCNセットアップ ・OCN実務研修 ・OCN合格者研修	実務研修カリキュラム ・機器設定 ・販売 ・応対マナー ・模擬応対 ・WBT試験 ・実技試験 ・合格者研修	合格者研修カリキュラム セキュリティ研修 ・セキュリティとは ・個人情報とは ・日常業務における注意点と対策 ・セキュリティポリシー	ブラッシュアップ研修 ・新サービス内容の確認 ・新技術のサポートについて　等 ※ セキュリティ研修 →合格者研修と同様の内容（※） 今後の「.com Security Master」へのカリキュラム準用に向け準備

2．トータルセキュリティを推進する三位一体の考え方

”人“、”プロセス“、”テクノロジー“といった三つの観点からセキュリティ・マネジメントの具体的対応策を検討し、テレワーク環境における「トータルセキュリティ」 を確立していくことが必要



3－1．テレワーク環境におけるセキュリティリスクと対策

・業務の妨害　(スパムメール、ネットワークの過負荷etc)
・スパイウェア、共有ソフトなどによる企業情報の漏洩

OS・アプリの脆弱性

・企業情報の漏洩
・データの改ざん、なりすましによる業務停止、妨害、不正利用
・踏み台にされた企業への攻撃により損害賠償のリスク

ウイルス・ワーム

不正アクセス
不正侵入

インターネットなど

FW

テレワーク端末

ネットワーク環境

社内リソース

端末の紛失・盗難

業務外利用

・紛失盗難や覗き見などにより顧客情報が漏洩した場合の企業責任、社会的信用の失墜

情報漏洩

・サーバ、ネットワークリソースの圧迫、追加設備投資によるコスト増
・企業ブランドの低下

3－2．テレワーク環境におけるセキュリティリスクと対策

区分	リスク	対策例
ネットワークに関するもの	不正アクセス、不正侵入	攻撃や不正アクセスから内部のネットワークを保護するファイアウォール。 不正なパケットを発見した時にアラームを表示し、通信ログを収集する侵入検知（IDS）や通信を遮断する侵入防御システム（IPS）、専任運用担当者の配置（24時間365日）
	ウイルス・ワーム	ウィルスやワームを検出して駆除するウイルスソフト、ウィルスゲートウェイ。 ウィルス情報などをテレワーカーに周知して注意を促す一斉配信システム
	通信経路上での盗聴	暗号化で盗聴を防ぐをSSL/IPSecVPN、通信事業者提供の閉域網
システムに関するもの	OS、アプリケーションの脆弱性	Windows Updateやセキュリティパッチのバージョンをチェックし最新化する検疫／回復システム、セキュリティパッチの準備、配布、適用、適用状況確認を行うセキュリティパッチ管理サービス
人為的なもの	機密情報漏洩	ソフトウェアやPC設定状況などを管理して不正利用監視する資産管理ソフト。 接続する本人を認証するワンタイムパスワード認証、バイオメトリックス認証 CPUやHDDのシリアル番号を識別して不正な端末からの接続を拒否するPC機体認証、インストールされているAPやレジストリの状態を識別し会社貸与以外のPCの接続を許可しないPC状態認証。USBキーなど外部メディアへの不正コピーを防ぐ情報漏洩対策ツール、PCに情報を残さないサーバサイドコンピューティング
	業務外利用や悪用	社内ポリシー策定、情報セキュリティ教育、職務に応じたアクセスコントロール、メールのフィルタリング、要注意人物の監視（ログ監視etc）
物理的なもの	盗難・紛失	PCのハードディスクを暗号化して閲覧を阻止するHDD暗号化ソフト、設置場所へのアクセス制御、施錠、管理簿記帳

4－1．eワーク（在宅勤務）のコンセプトと導入ステップ

導入目的

個々人がやり甲斐のある仕事にチャレンジできる仕組み作り」の一環として、多様なワークスタイルの実現を目指す

1．ワーク・ライフバランス向上、ワークチャンス拡大

2．NTT-ComのIPサービスを使ったビジネスモデルの実践・提案

HRMの3本柱

導入ステップ

“eベース”のワークスタイルの定着

STEP1（2002年度）
○試行的位置づけで実施
○在宅勤務日数：週1～2日
○実施期間：半年程度

STEP2（2003年度）
STEP1の実施結果を踏まえ、拡大実施

STEP by STEP
で拡大し、ノウハウを蓄積しつつ、ワークスタイルの選択肢の1つとしての定着を目指す

STEP1の実施概要（2002年11月～半年間）

対象者	主な実施業務／実施環境
計20名 ・開発系の業務に従事する社員（15名） ・育児のための短時間勤務の社員（5名）	・アーキテクチャ開発業務における仕様検討、技術資料の作成 ・ユーザ案件販売支援業務における提案書、システム設計書等の作成　等 ・**『ICカード』等を利用し、セキュリティを担保した社内LAN接続**

STEP2の実施概要（2003年11月～）

対象者	実施環境
計50名程度 ・自立的に業務を遂行できる社員 ・育児・介護のための短時間勤務の社員 ・身体に障害を持つ社員	・『ICカード』等を利用し、セキュリティを担保した社内LAN接続 ・**セキュリティ・ポリシーの遵守** ・セキュリティの観点から、会社で管理する**「IT一元化PC」を使用**

4－2．eワークの運用イメージ

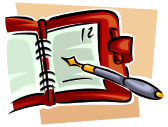
eワーク実施場所

事前に提出の実施プラン基づき、業務を実施

【勤務時間例】
＝所属組織の勤務時間と同じ
9:00始業　　17:30終業
昼食

前日まで

実施プランの提出



eワーク実施日

始終業時刻・作業場所の連絡

指示・フィードバック

ｱｳﾄﾌﾟｯﾄの提出

出社

※eワーク実施日でも上長からの要請があったときは出社

会社

直属上長

職場

会議

ベンダ打ち合せ

社内リモートアクセスセキュリティ対策

【外部からのｳｲﾙｽ進入、端末乗取りおよび不正アクセスの防止】

社外から

インターネット

IPsec暗号路

※利用者の必須条件

セキュアゲートウェイ

認証ﾌﾟﾗｯﾄﾌｫｰﾑ

IPSec GW

FW＆IDSｻｰﾊﾞ

ﾘﾊﾞｰｽﾌﾟﾛｷｼ

専用線

社内ネット

許可されていない社内Webｻｰﾊﾞ

許可された社内Webｻｰﾊﾞ

対策①

①ICカードによる厳密な本人認証

②不正アクセス対策
・ｳｲﾙｽ対策＆ﾊﾟｰｿﾅﾙFWの導入
・Webｻｰﾊﾞ（IIS等）の導入禁止

対策③

③ ﾘﾊﾞｰｽﾌﾟﾛｷｼによる対策
・httpのみを通信許可
・ｳｲﾙｽの進入を防止

対策④

④アクセス制御機能により指定された業務AP（Web）のみを接続