デジタル通信技術概論　第5回

①・端末設備の運用/保守管理技術
通信網の運用/保守管理は、それを使用する立場からしても非常に重要な問題であり、ひいては個人レベルのLAN環境の運用/保守管理にもこの知識を役立てることができる。

②・情報セキュリティ関連法案とリスクマネジメント
現在の我が国における情報セキュリティ関連法案とリスクマネジメントついて学び、個人レベルでのセキュリティ対策に役立てる。

端末設備の運用/保守管理技術

端末設備の運用状態は、大きく３つに分けることができる。

通常時運用：通常に運用されている状態
障害時運用：何らかの障害が発生し、通常とは異なる状態で運用し続ける状態
保守：メンテナンスやシステム拡張などの変更作業

運用/保守管理項目としては、以下のものが考えられる。

管　理　項　目	内　　容
構成管理	端末設備の構成要素の状態監視に関する管理
障害管理	障害に関する管理
性能管理	全体の性能指標を中心とした管理
安全性管理	セキュリティ・信頼性に関わる管理
設備管理	端末設備の設置環境（ファシリティ設備）に関する管理
課金管理	通信料金などに関する管理

構成管理

設備を構成する機器や配線を、それぞれの結びつける状態およびその稼動状態などを把握し、管理する。

①・対象管理
構成要素（機器や通信回線）別に属性や制御情報といった個々のデータを管理し、これをもとに設備への追加や削除を行う。
最新の情報を常に現行化して最新の情報を保つようにする。

②・関係管理
構成要素間のつながりを管理する。
構成要素の管理がしやすくなるような要素間の関係を保つようにしなければならない。

機器番号・アドレス

③・状態管理
付帯設備、通信回線を含む全てのネットワーク構成要素について、現在の状態を収集、監視する。

稼動状態の把握・総トラヒック量

障害管理

機器や通信回線に障害が発生した際に、その検出方法や対策、さらに予防の方法を検討して実行する。

①・障害検出管理
障害に対する対応を迅速に行うために、障害に至る前段階の状態にある設備の動作記録が、ある一定レベル以下になった場合にエラー勧告を発生させるなどの機能を準備する。

②・障害試験管理
ループバックや自己診断機能などの手段による、障害発生時における障害発生個所切り分けの機能を準備する。

③・記録制御管理
障害の原因を究明するために、ネットワークの統計情報や機器からのメッセージ、利用時間などの記録情報（ログ）を収集して分析する。

④・障害報告

障害が発生し、原因が特定され問題が解決したら、運用管理者は必ず各関係者へ報告する必要がある。

障害報告の内容

- 障害発生時間
- 復旧時間
- 対応時間
- 障害内容
- 影響範囲
- 今後の対策と対応後の設備環境の変化について

今後の対策を検討する場合は、
情報を統括するアドミニストレーターとの
話し合いを持つ。

その他の管理要項

性能管理
設備全体に関する性能情報、回線に接続される機器に関する性能情報、信頼性に関する情報、統計情報などを管理する。

安全性管理（セキュリティ管理）
設備を何からどのように守るかを考慮し、実行する。
インターネットに接続されるシステムである場合には、不正アクセスやウイルスへの対策を講じる必要がある。

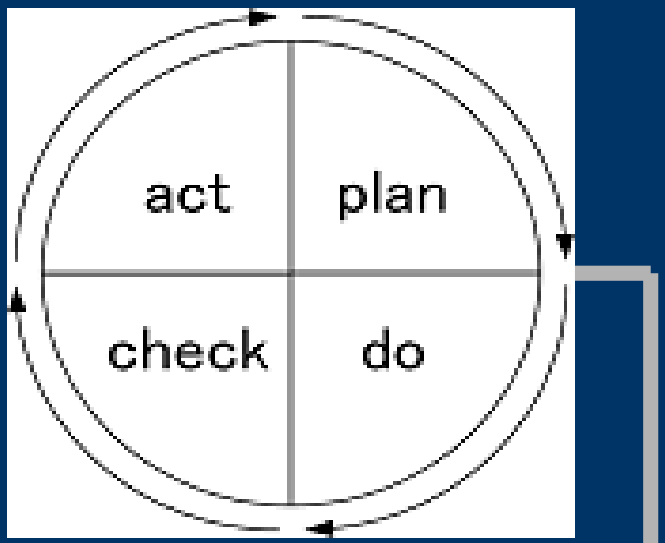
設備管理
通信設備以外に通信設備を利用するために必用な電源や、機器を設置している環境に関する設備などを管理する。

課金管理
通信料などの金銭面の管理。

情報セキュリティ管理

情報セキュリティを確実にするためには、組織トップの関与を確実にした管理を実施し、組織としての情報セキュリティポリシーを確立し、リスクマネジメントに基づく費用対効果を考慮したセキュリティ対策を計画し実施する。

PDCAサイクルによる情報セキュリティ管理のプロセスアプローチ
P→Plan(計画)
D→Do(実施、実行)
C→Check(評価、点検)
A→Act(改善、処置)



input
利害関係者の情報セキュリティ要求事項及び期待

output
運用管理された情報セキュリティ

情報セキュリティ管理の確立

１・情報セキュリティ基本方針の確立

情報セキュリティに対する要求事項を考慮し、全般的な方向性（行動指針）を確立し、企業においては経営陣の認証を得る。

影響

・リスクマネジメント環境
・情報セキュリティ管理を確立する組織環境

２・リスクアセスメントに基づく管理策の選択

決定した情報セキュリティ基本方針に基づき、リスクアセスメントの体系的な取組方法を策定する。

リスクの識別･･･機密性、完全性、可用性に対する脅威と脆弱性およびそれら事業に及ぼす潜在的な影響力の識別

リスクアセスメント･･･セキュリティ障害の発生による事業上の損害と可能性から、そのリスクの度合いを算定し、リスクの受容と対応が可能かどうか判定を行う。

リスク受容不可→リスク対応（リスク回避/移転/保持）

リスク対応の結論に従って、適切な管理目的と管理策（セキュリティ対策）を決定する。

３・リスクについて適切に対応する計画の策定

管理目的および管理策、さらにその理由を記載した適用宣言書を作成し、経営陣より認証を得る（経営陣による残留リスクの把握）。

情報セキュリティ管理の実施

リスクマネジメント

リスクを受容可能な水準にまで軽減するためのリスク対応方針および目標を設定するとともに受容可能なリスクの水準を特定する。

１・情報資産の洗い出し

情報資産の保有状況を調査し情報資産目録を作成する。
資産価値や属性が同じものは、グループ化してまとめて管理する。

２・リスク因子の特定

情報資産が曝される脅威と、管理上の問題などによる脆弱性の組み合わせでリスクが顕在化する。

脅威の洗い出し→人為的脅威、自然的脅威などの脅威の識別
脆弱性の検討→脅威発生を誘引する情報資産固有の弱点やセキュリティホールなどの識別と検討

脆弱性は、それだけでは何ら障害とならない。
脅威を顕在化させ、損害や障害を導く可能性がある。

３・リスク値の算定

リスクを数値論理的に評価し、受容できるか、対応が必要かを決定する。リスク値は、各項の積によって求めるのが一般的である。

（例）
リスク値＝脅威の大きさ×脆弱性の度合い×情報資産の価値
リスク値大→受容/対応の検討
　　小→受容

４・リスク評価

リスク対応が必要なリスクについては、リスク対応計画を策定し、必要なセキュリティ対策を実施する（リスク対応）。
技術の進歩は新たな脅威や脆弱性を生み出し、リスクは時間と共に増大する。リスクに対する適切なセキュリティ対策とコストを識別し、定期的に見直すリスクマネジメントが必要である。

（例）
PDCAモデルで定期的に見直すようなリスクマネジメント

５・リスク対応

リスクアセスメントで明確にされた管理対象となるリスクに対して、実際に対応を行う。対応方法は以下の４つに分けられる。

最適化

ISO/IEC27001付属書による127項目の管理策の適用や追加の対策の実施。リスクの発生確率の低減、リスクの受容可能な水準までの低減。

保有

あるリスクが受容のための評価基準を明らかに満たす場合、そのリスクを受容する。

回避

リスク対応の検討を行ったうえで、コストに対応した利益が得られない、適切な対応策が見出せないなどの場合において、そのリスクがある情報資産を破棄する。

移転

契約などによりリスクを他者に移転する。アウトソーシングや保険などの方法があるが、リスクの移転に際し、そうした場合のリスクを再検討する必要がある。

導入と運用

情報セキュリティ基本方針、管理策、プロセスおよび手順を導入し運用する。

リスクを管理するためのリスク対応計画を策定し実施する。
・運営人の適切な行動
・責任および優先順位
・残留リスクへの追加対策
・管理策の運用に関する手順
・セキュリティ事故や事件発生の際の手順

明文化

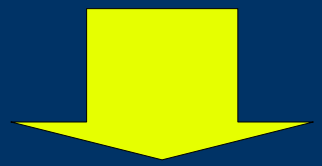
経営陣による経営資源の提供

情報セキュリティを認識させる教育や訓練等のプログラムを実施する。その有効性を評価し、実行可能な資格・能力を持つ要因を確保する。

監視と見直し、維持および改善

情報セキュリティ管理を監視および見直す。

- プロセスの実施状況を評価、測定し、経営陣に報告
- 管理の有効性について定期的な見直し
- リスク水準の見直し
- 定期的な内部監査の実施



これまでの経験から学んだ教訓を活用する

情報セキュリティ管理を維持および改善する。

- 予防措置および是正措置を講ずる。
- 講じた対策を伝達し、改善目標を確実に達成する。

利害関係者全てから、可能な限り合意を得る

個人情報保護

個人情報保護法

→個人情報取扱業者における義務と責任の発生

- 利用目的の明確化
- 適正な取得
- データ内容の正確性確保
- 安全性の確保
- 本人の求めに応じた対応

電気通信事業における個人情報保護に関するガイドライン

通信の秘密に属する事項その他の個人情報の適正な取扱いに関し、電気通信事業者の遵守すべき基本的事項（個人情報保護法に沿う）

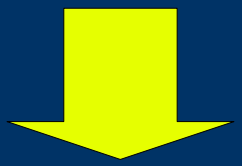
- 収集にあたり目的の特定
- 適正管理
- 情報主体からの求めにより開示・訂正
- 責任の明確化
- 通信の秘密に関する個々の情報等の規定

個々の情報等の規制

①・通信履歴の記録→課金、料金請求などの業務遂行に必要なものに限定
②・利用明細→目的内に限定
③・発番号通知→個人情報通知阻止機能の持つこと
など

情報通信ネットワーク安全・信頼性基準(S62郵政省告示)

①・個人情報へのアクセスの管理
②・個人情報の持出し手段の制限
③・外部からの不正アクセス防止のための措置



安全管理措置

法的適合性

情報セキュリティ管理に関する法律の適用

①・民事法（民法）関係
→民法：物件、債権、相続など
→商法：会社法、商行為法、海商法など

②・行政法関係
→商標法、特許法、著作権法など

③・刑事法（刑法）関係
→不正競争防止法、不正アクセス禁止法など

④・知的所有権法関係
→税法、電気通信事業法、独占禁止法など

憲法

表現の自由と通信の秘密を規定

第二十一条
集会、結社および言論、出版その他一切の表現の自由は、これを保障する。

２　検閲は、これをしてはならない。通信の秘密は、これを侵してはならない。

不正アクセス禁止法

不正アクセス行為の禁止等に関する法律

→不正アクセス行為の禁止
→行為に対する罰則およびその再発防止を図る

第三条
何人も、不正アクセス行為をしてはならない
→不正アクセスの禁止

第四条
（略）識別符合を管理者及び利用権者以外に提供してはならない
→不正アクセス行為を助長する行為の禁止（違反した場合、三十万円以下の罰金）

第八条
次の各号の一に該当する者は、一年以下の懲役又は五十万円以下の罰金に処する。
一　第三条第一項の規定に違反した者
二　第六条第三項の規定に違反した者

その他の法律

電子署名及び認証業務に関する法律（電子署名法）
→電子署名の信頼性及びその価値について規定

電子通信事業法
→通信の秘密の保護

刑法（関連条文）
第175条：わいせつ物配布
第230条：名誉毀損
第246条：詐欺

電波法
→無線局の開設と秘密の保護のより詳細な取り決め

有線電気通信法
→通信妨害や回線使用に関する罰則

以上です。お疲れ様でした。

その他の法律については専門書や弁護士をご利用ください。