ユビキタス環境における企業ネットワーク構築
－内部統制への布石となる導入指針－

アブストラクト

1. 研究の背景

ユビキタスネットワークとは、一般に「いつでも、どこでも、何とでもアクセスが可能であるネットワーク環境」といわれており、昨今の ICT(Information and Communication Technology) の進歩により、その実現が技術的には可能になりつつある。しかし企業活動を支える企業ネットワークでは、信頼性の確保や社内ルールへのコンプライアンス等の要件を満たす必要があり、導入効果やセキュリティに対する課題等、漠然としたユビキタス環境の導入検討が進みづらい状況である。

2. 研究の目的と進め方

当分科会では、個人情報保護法の施行や日本版 SOX 法の制定を理由にユビキタス技術の導入に消極的な企業に対し、ネットワークのユビキタス化を提案し、慢性的な人員不足の解決や、生産性を高める手段を提供することを目的とした。その際、企業ネットワークのユビキタス化を成功させる鍵は、ユビキタス技術の選択方法や導入方法ではなく、導入後に発生する問題に対して、事前に対策を立てておくことにあると考えた。

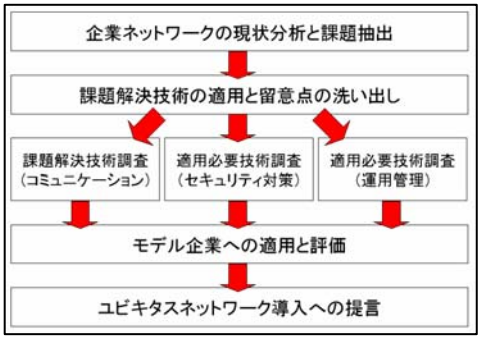


図 1 研究の目的と進め方

そこで我々は、(1) ユビキタス技術によるコミュニケーションの強化、(2)ユビキタス化で発生する新たなセキュリティリスクへの対処、(3)企業活動を把握するための管理手法の確立、の３つを提案し、モデル企業を使って具体的な実現手法を示した。(図１参照)

3. 研究成果

(1)ユビキタス環境を導入するための企業ネットワーク構築手法

①コミュニケーション強化の提案

■コミュニケーションのボトルネックの分析

「人－人」のコミュニケーションのボトルネックは、「人－モノ」「モノ－モノ」のコミュニケーションのボトルネックにより発生すると分析した。(表 1 参照)

表 1 コミュニケーションのボトルネック事例

事例	「人－モノ」のボトルネック	「モノ－モノ」のボトルネック
電話をかける場合	①名刺や電話帳等使用し電話番号を調べる。 ②電話番号をプッシュする。	相手が不在の場合には、改めて電子メールで用件をキーボードで打ち直す。

■コミュニケーションの改善手法の提案

ボトルネック解消案のひとつとして SIP/Web 技術を活用し、プレゼンスと連動したサービスを行うことで、上記の問題が解決できることを示した。(表 2 参照)

表 2 コミュニケーションの改善例

事例	「人－モノ」の改善手法	「モノ－モノ」の改善手法
電話をかける場合	メールのクリックにより、そのメールの発信者へ電話がかけられる。(Click-to-Call)	相手の不在時には、こちらの音声が自動的に電子メールの添付ファイルとして相手に送信される。(Voice Mail)

②セキュリティ対策の提案

■現行のセキュリティ対策の課題分析

現行のセキュリティ対策の課題を「物理的なセキュリティの限界」「セキュリティゲートウェイ（ファイアウォール）による対策の限界」「従来のアンチＸ（ウイルス対策ソフト）の限界」「人による管理の限界」に分類し、対処策を提案した。(表 3 参照)

表 3 現行のセキュリティ対策の課題（検討結果）

検討項目	課題
セキュリティ対策	①無線 LAN への不正アクセス。(物理的なセキュリティの限界) ②感染PCの持ち込み。(セキュリティゲートウェイの限界) ③P2P ソフトの不正使用。(従来のアンチXの限界) ④ネットワーク型ワームの大規模感染。(人による管理の限界)

■企業ネットワークのユビキタス化に対応したセキュリティ対策の提案

ユビキタス化に備えるために行っておく対策として「論理的なセキュリティ境界の構築」「未知の脅威への対策」「大規模感染の抑制」を提案し、具体的な構築手法を示した。(表 4 参照)

③企業ネットワークの運用管理手法の見直し提案

コミュニケーションの改善により、トラフィックが SIP／Web に統合される。このため SIP／Web トラフィックを詳細に分類すべく管理レベルを上げ、トラフィックの可視化が必要となることを提案した。

表 4 セキュリティ対策の提案（検討結果）

検討項目	提案内容
セキュリティ対策	①ネットワークの全ての入り口に「認証」「監査」「アクセス制御」を実装する。(論理的なセキュリティ境界の構築) ②端末にはシグネチャ情報に基づかない「ふるまい監視」機能を導入する。(未知の脅威への対策) ③ネットワークインフラにはウイルスシグネチャ情報に基づく動的フィルタリング機能を付与する。

(2)モデル企業におけるユビキタス技術適用における課題と考慮点の明確化

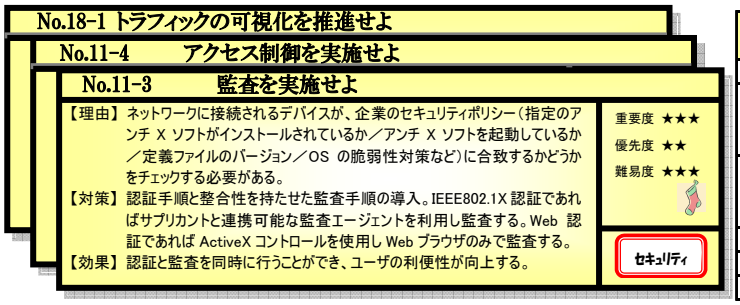
企業において導入が検討されつつあるユビキタス技術のうち「無線 IP 電話」「プレゼンス」「検疫ネットワーク」の３つの技術について導入構築時の適用課題と考慮点を導き出した。(表 5 参照)

表 5 ユビキタス技術導入構築時の課題と考慮点

	無線 IP 電話	プレゼンス	検疫ネットワーク
技術適用時の課題	PC と無線 IP 電話機の認証レベル不一致により不正アクセスが発生する原因となる。(IEEE802.11e を利用したネットワーク統合時の課題)	手動管理の手間により、プレゼンス機能が有効活用されなくなる。	IEEE802.1X 認証／Web 認証の認証方式を規模や環境に合わせて選択する必要がある。
課題に対する構築時の考慮点	データと音声の VLAN 分割や音声ネットワーク上でのアクセス制御が必要である。	入退出管理システム、スケジューラ、ネットワーク接続状況等との連携による自動更新と手動更新を併用する必要がある。	守るべきネットワークエリアを明確化し、導入計画に沿った一括導入／段階的導入を見極める必要がある。

(3)ユビキタス環境導入に向けた企業ネットワーク検討指針集（６０鉄則）

ネットワーク管理者の意見を基に管理者のノウハウを集約させた、企業ネットワークのユビキタス化準備のためのネットワーク検討指針とチェックシートを作成し、更には日本版 SOX 法と関連のある項目については関連性を示した。(図 2 参照)



No		検討内容	チェック 担当者	チェック 管理者
5	5-1	「人-人」のコミュニケーションの実態を確認せよ	□	□
11		論理的なセキュリティ境界を構築せよ	□	□
	11-3	監査を実施せよ	□	□
	11-4	アクセス制御を実施せよ	□	□
12		未知の脅威への対策をせよ	□	□
	12-1	使用禁止アプリケーションを検出せよ	□	□
	12-2	ふるまい検知・ブロック機能を利用せよ	□	□
13		大規模感染の抑制に対する準備をせよ	□	□
18	18-1	トラフィックの可視化を推進せよ	□	□
23		企業制度の見直しを検討せよ	□	□

図 2 ユビキタス環境における企業ネットワーク検討指針集と確認チェックリスト

4. 「ユビキタス環境における企業ネットワーク構築」における４つの提言

■提言１　ユビキタス化することは内部統制（日本版 SOX 法対策）にもつながる

ユビキタス環境では認証の強化、アクセス制御、更にはネットワークのアクセス状況、手順、行為等を管理するログの取得が必要とされる。これらの行為は内部統制でも必要とされている。つまりユビキタス環境を企業ネットワークに導入することは、内部統制への準備を行うことにもつながる。

■提言２　コミュニケーションを連携させ、ゆとりのある職場環境と時間を生み出せ

「人ー人」「人ーモノ」「モノーモノ」のコミュニケーション連携により、あらゆる場所で同じコミュニケーションレベルを維持した職場環境のゆとりと、時間のゆとりを生み出す。この環境や時間のゆとりにより従業員をメンタル面でサポートし、従業員満足度の向上が企業の競争力強化につながる。

■提言３　「点」のセキュリティから「面」のセキュリティを導入せよ

従来のファイアウォールや端末等、点在する機器での「点」のセキュリティ対策から、ネットワークの入り口で「認証」「監査」「アクセス制御」についても行う「面」のセキュリティ対策が重要となる。つまり従来の対策に加え、「論理的なセキュリティ境界を構築する」ことが求められる。

■提言４　企業ネットワークの重要性と管理すべきことへの意識を変えろ

RFID を活用した「モノーモノ」通信等による情報機器の増加、更にはそれらのトラフィックにおいて SIP／Web の活用が主流となる。ネットワークトラフィックを詳細に分類するため管理レベルを上げ SIP／Web 上で行われている具体的な通信の分析が求められる。つまり企業ネットワークの重要性が増していることを認識し、管理すべきことを改めて見直し、それらに対する意識を変えるべきである。

5. まとめ

今後、企業ネットワークは複雑化し重要度が増す。情報システム部門は運用管理が複雑化するため、経営的な視点や広い視野が要求される。一方、経営者は情報システム部門の立場、役割、責任などを明確に位置付け、有効に機能するためのビジョンを示す必要がある。