建築現場事務所のIT環境の標準化

（株）朝日工業社

■ 執筆者Ｐｒｏｆｉｌｅ ■

牧瀬博詔

1989年　(株)朝日工業社　入社
システム業務担当
1994年　工事現場業務担当
2005年　現在 情報システム室所属
システム業務担当

長堀秀之

1992年　(株)朝日工業社　入社
技術情報管理業務担当
1994年　現在 情報システム室所属
システム業務担当

■ 論文要旨 ■

近年，公共投資の減少，建設コストの低減要求，工期の短縮要求などにより，建設現場全体の生産性向上，コスト低減が求められており，その手段として現場内のＩＴ化が進展しているが，一方でセキュリティのリスクが増大している．

現場の要求を分析してアクセス要件をまとめ，安価な機器の組合せで現場事務所のＩＴ環境を標準化することで，現場の効率化要求を損なわずに，セキュリティの向上を実現した．

■ 論文目次 ■

■ 図表一覧 ■

１．はじめに

１．１　当社の概要と建設現場の特徴

当社は資本金 38 億円，従業員数約 900 名の空調・衛生設備の施工管理を主とする建築設備工事業者である．

建設現場は全国各地に点在しており，当社社員が常駐している現場は常時 300 ヵ所前後が存在する．建築物の施工は建設会社（以下　「ゼネコン」という）を中心に当社のような設備工事業者，および，各社の協力業者等が協力しながら行われる．

工期は建物の規模や用途により，短いものは数ヵ月，長いものは３年をこえる．平均すると約１年ぐらいである．

現場ではゼネコンを主軸に，当社を含めた設備工事業者を少なくとも２～３社加えた構成で仮設事務所を作って同居している．

当社の事務所には当社の社員の他に，派遣会社からの出向社員，協力業者の社員など，外注社員と呼ばれる当社で管理すべき人員が常駐している．

２．背景

２．１　現場事務所の効率化要求

近年，公共投資の減少，建設コストの低減要求，工期の短縮要求などにより，建設現場全体の生産性向上，コスト低減が求められている．その手段としてＩＴ化が進展し，現場内に下記の目的でネットワークを構築する現場が増えてきている．

(1) プリンタ，プロッタなどの共同利用．

小規模な現場事務所では空調設備，衛生設備，電気設備の設備工事業者が１部屋を共同で利用する事が多い，その場合，事務所の省スペース化，コストの低減の為にプリンタ，プロッタなどの共同利用が必要である．

(2) 情報の共有

ＣＡＤデータ等の他社への受け渡しや，議事録，工程表，日報等の書式，共通資料の現場全体での共有，施工写真，ＣＡＤデータ，施工関連資料等の当社内部での共有が必要である．

(3) インターネットの利用

メーカーのホームページからの機器や材料のＣＡＤデータのダウンロードや，メール等の送受信の為に，インターネットが必要である．

２．２　社内ネットワークへの接続要求

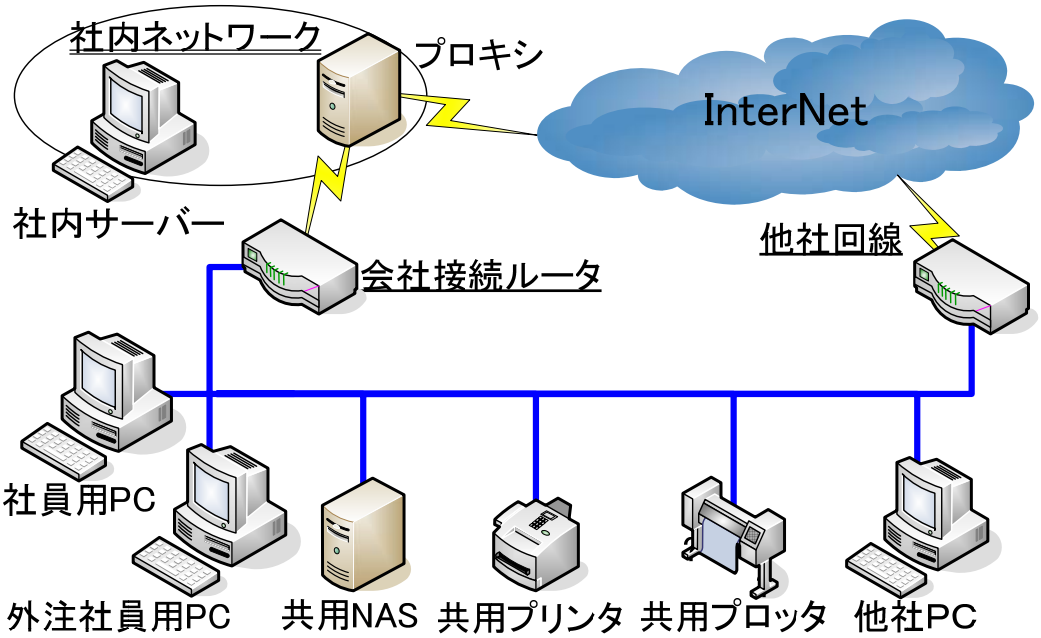
当社の基幹システムは，現場の担当者も含めた全社員が社内のサーバーに接続して使用する．又，全社員向けの通達や個人宛のメールも社内のサーバーに集積されているため，当社社員の使用するパソコン(以下 PC という)は社内ネットワークへの接続が必須である．

２．３　現場事務所のＩＴ環境と問題点

上記の要求に対し，各現場ではネットワークを不慣れな社員が試行錯誤して構築するか，専門会社に依頼するなどして，個別にＩＴ環境を構築している．そのため，現場のＩＴ環境は構築する者のセキュリティ意識やネットワークスキル，現場の事情などによって多種多様となっている．

図１は当社の現場で多く採用されているネットワーク構成である．ネットワーク上に当社社員用 PC，データ共有のための LAN 直結型ハードディスク（以下 NAS という），共同利用のプリンタ，プロッタ，社内接続やインターネット接続のためのルータなどが接続されている．

図１　現場のネットワーク構成例



現場によりネットワーク構成に違いはあるが，他社のＰＣと同じネットワークに当社のＰＣが接続されている状況はどの現場でも同様で，それらのＰＣを経由したウイルスの攻撃や不正侵入，Winny などによる情報漏洩の危険がある．

現場で扱うデータ容量は平均 20GB 程度になるが，データのバックアップ方法，利用メディアなどの方針は確立していない為，バックアップは現場の自主性に任され確実ではない．

この状況をまとめると問題点は下記のようになる．

(1) 共有領域から社内ネットワークへの不正侵入
(2) 社員用パソコンおよび社内ネットワークへのウイルス攻撃
(3) 現場内データの盗難，火災，故意による消失

ＩＴ化の進展により現場の書類のほとんどが電子データ化されている為，消失や漏洩があった時の被害は大きいが，本来，重要なデータ保全に関する問題は効率化要求に比べて軽視されている．

２．４　原因と対策

このような問題が発生するのは下記の原因による．

(1) ＩＴ環境の構築方法が確立されていない．

当社の規定では現場で他社とネットワークを接続する事は禁止しており，他社との接続を前提とした安全なＩＴ環境の構築方法は確立されていない．

(2) ＩＴ環境の構築スキルを備えた人員の不足．

構築方法が確立されても年間 300 ヵ所前後が新設される現場事務所のネットワークの構築を行うためには，ネットワークスキルを持った人員が不足している．

(3) 現場担当者のセキュリティ維持管理のスキル不足．

現場では外注社員の増員，減少が頻繁に起こる為，ＰＣ等の追加，変更が必要になるが，現場担当者が行うとスキルが低いためセキュリティ低下の危険がある．

以上を改善する為には，ＩＴ環境の構築方法を確立し，それを全現場で使えるように汎用化し，維持管理にネットワークスキルがいらないように簡略化する必要がある．

汎用化，簡略化のためには，機器や環境を統一する事が最も有効な方法であると考え，現場ＩＴ環境の標準化に取り組むことになった．

３．標準化への取り組み

３．１　要求の分析

３．１．１　不正アクセスの防止

不正アクセスを防止するには利用者が必要とするリソースを把握し，許可すべきリソースを決定する必要がある．そこで，現場にいる人員を，当社の「社員」，当社で管理すべき「外注社員」，当社の管理が及ばない「他社」と分類し，効率化要求に従ってリソースの利用形態を分析すると表１のようになり，利用形態ごとにリソースを，全利用者が必要とする「共有リソース」，社員と外注社員が必要とする「当社リソース」，社員のみが必要である「社員リソース」，に分類できる．

表１　利用者が必要としているリソース

利用者	リソース				
	プリンタ，プロッタ	現場全体の共通資料	当社現場内データ	インターネット	社内ネットワーク
社員	必要	必要	必要	必要	必要
外注社員	必要	必要	必要	必要	禁止
他社	必要	必要	禁止	禁止	禁止
分類	共有リソース		当社リソース		社員リソース

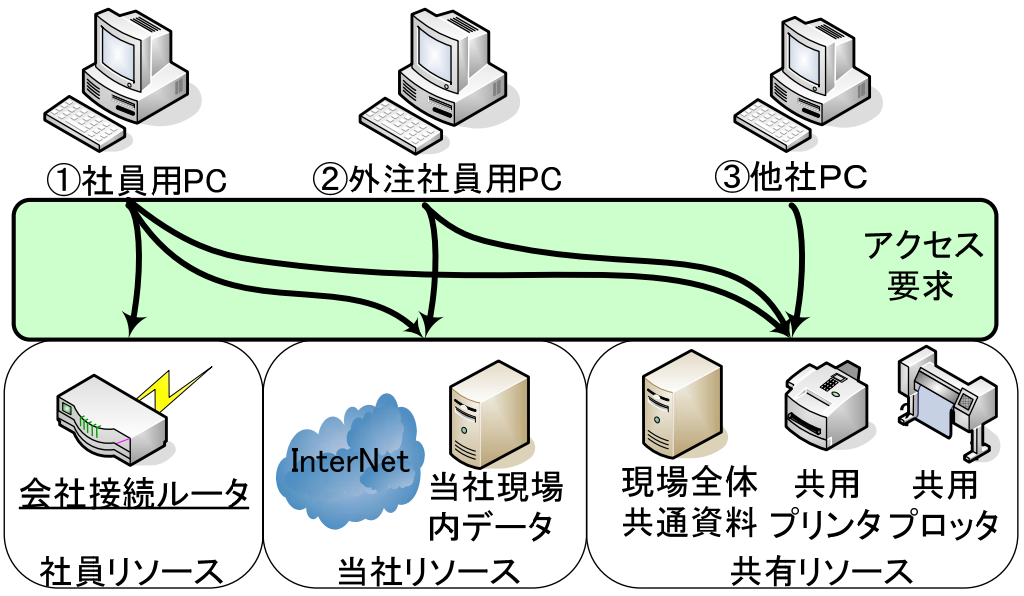
不正アクセスの防止は利用者の使用する PC とリソースを下記のようなアクセス制御を行う事で実現され，まとめると図２のようになる．

① 社員用ＰＣから共有リソース，当社リソース，社員リソースへのアクセス許可

② 外注社員用ＰＣから共有リソース，当社リソースのアクセス許可と社員リソースへのアクセス禁止

③ 他社ＰＣから共有リソースのアクセス許可と当社リソース，社員リソースへのアクセス禁止

図２　必要なアクセス



３．１．２　ウイルス対策

ウイルスの対策方法としては下記が考えられる．

- 新規ウイルスの進入阻止
  - コンテンツフィルターによりウイルスダウンロードサイトへのアクセスを防ぐ
  - 感染の可能性のある危険なＰＣからのアクセスを防ぐ
- ウイルスの早期発見，駆除
  - 対策ソフトを最新の状態に保ち，定期的にウイルス検索を行う．
- ウイルスの活動の阻止
  - コンテンツフィルターにより，自己アップデートサイトへのアクセスを防ぐ
  - プロキシを経由することにより，バックドアからのアクセスを防ぐ

この対策は下記の要件を満たすことで実現される．

(1) インターネットの利用は社内のプロキシを経由してコンテンツフィルターを通す．
(2) ネットワークセグメントを分けてアクセス制御を行い，他社ＰＣから当社ＰＣへのアクセスを防止する．
(3) 対策ソフトを最新の状態に保ち，定期的にウイルス検索を行う．

３．１．３　データ消失対策

データ消失対策に最も有効な方法は，データバックアップであり，要件は下記による．

(1) 不在時や忘れの防止のためにバックアップを自動実行する．
(2) 確実にバックアップが取れたか，本社で確認をする．
(3) バックアップされた媒体を取外し，盗難や火災など，災害の影響を受けない安全な場所へ保管する．

3．1．4　導入運用に関する要求

各現場に導入を促し，セキュリティ上危険な状態の現場をなくす為には導入運用に関して，以下の要件が必要になる．

(1) 安価な予算で導入できる．

(2) 現場事務所開設時に速やかに納品できる．

(3) 導入，設置，環境構築が簡単である．

(4) トラブル時の対応が速い

- 中央からの遠隔操作により障害の切り分けができる．
- 機器が故障してもバックアップデータの利用により，業務を止めない．

3．2　実現手段

3．2．1　アクセス制御とセグメント分割

以上の要件を満たす手段としてアクセス制御方法の選定が重要となる．

ウイルス対策のためには「3.1.1 不正アクセスの防止」の図２「必要なアクセス」で分けたグループを，ユーザー認証などのソフト的な手法ではなく，それぞれセグメントで分ける必要がある．

セグメントを複数に分ける方法として，ファイヤーウォール機能を持つ機器を使用すると，「ＰＣ」と「リソース」をセットにして，図３のようなアクセス制御でセグメントを構成することができ，現場での運用が簡単になる．

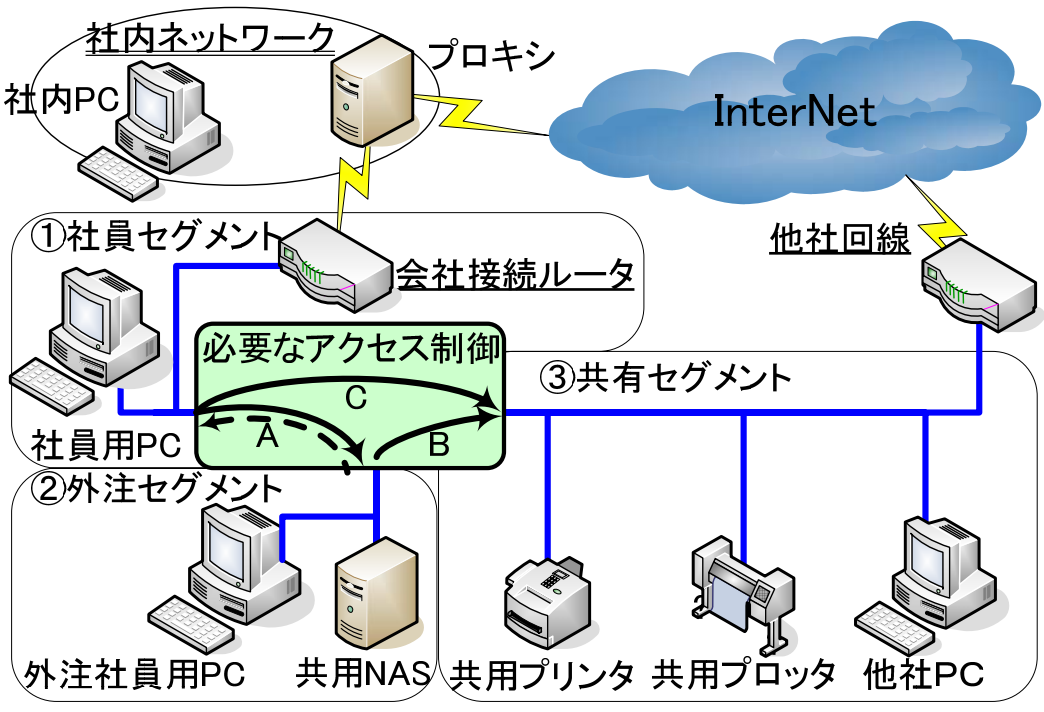
セグメントの組合せと名称は下記のように決めた．

① 社員ＰＣと社員リソースを同一セグメントにまとめ，「社員セグメント」

② 外注社員ＰＣと当社リソースを同一セグメントにまとめ，「外注セグメント」

③ 他社ＰＣと共有リソースを同一セグメントにまとめ，「共有セグメント」

図３　セグメント構成とアクセス制御



セグメントの制御方法としては表２に示す方法を検討した．

「インテリジェントスイッチによるＶＬＡＮ」方式と「PC に LAN ボードを複数装着」方式は要件を満たさず，「L3 スイッチ，３セグメントルータ」方式は高価である．

そこで今回考案したのは，セグメントを２分割するだけの安価なルータを２台組み合わせることで３セグメントに分け，アクセス制御を下記のように行う方法である．

(1) 社員セグメントから外注セグメントは参照できるが，逆方向のアクセスはインターネット利用時のプロキシ宛のアクセスのみを許可する．（図２のＡ）

(2) 外注セグメントから共有セグメントは参照できるが，逆方向のアクセスは全て不可とする．（図２のＢ）

※逆方向のアクセスを全て不可としないで，共用 NAS 宛のアクセスのみを許可する方法も検討したが，セキュリティホールが発生するため，他社とのデータの共有が必要な時は，共有セグメントにもう一台ＮＡＳを置く事とした．

(3) 社員セグメントから共有セグメントを参照する時は外注セグメントを経由し，それぞれのアクセス制御に従う．（図２のＣ）

各セグメントの IP アドレスについては，社員セグメントの IP アドレスは社内ネットワークと接続している IP-VPN で決定し，共有セグメントの IP アドレスは他社との協議で決定する．外注セグメントの IP アドレスは当社が任意で決められるので，全現場共通とし，ＩＰアドレスの標準化を行う．

表２　セグメント分割方法の比較

方式	セグメント分け	アクセス制御	ウイルス対策	価格
インテリジェントスイッチによるVLAN	△ 注1	△ 注2	△ 注3	○ 2～3万円
L3スイッチ，3セグメントルータ	◎	◎	◎	△ 10 万円以上
PCにLANボードを複数装着	◎	◎	× 注4	◎ 1 万円程度
2分割ルータを2台	◎	◎	◎	◎ 1 万円程度

注1)IPアドレス変換ができない

注2)ファイヤーウォール機能が無いので，図2のままのセグメントでアクセス制御になる．PC セグメントは互いのアクセスを禁止し，リソースセグメントに対してアクセスを許可する．

注3)リソースセグメントに誤ってPCやサーバーを接続すると危険である．

注4)セグメントを分けるPC自体がウイルス攻撃の対象となる．

３．２．２　サーバーの導入

ウイルス対策，データ消失対策などのセキュリティ対策を実現するため，サーバーを導入し，下記の対策を実行する．

(1) 日次でフルバックアップを行う．

(2) ウイルスチェックはフルバックアップ時にリアルタイム検索で行う．

(3) バックアップデータはポータブル型のＵＳＢハードディスクに退避して，着脱し盗難や火災などの災害の影響を受けない安全な場所へ保管する．このデータは共用 NAS やサーバーが故障した際に，一般的なＰＣで利用する．

(4) バックアップを確実にする為にバックアップタスクの最後でハードディスクの残容量をチェックし，中央へ報告する．

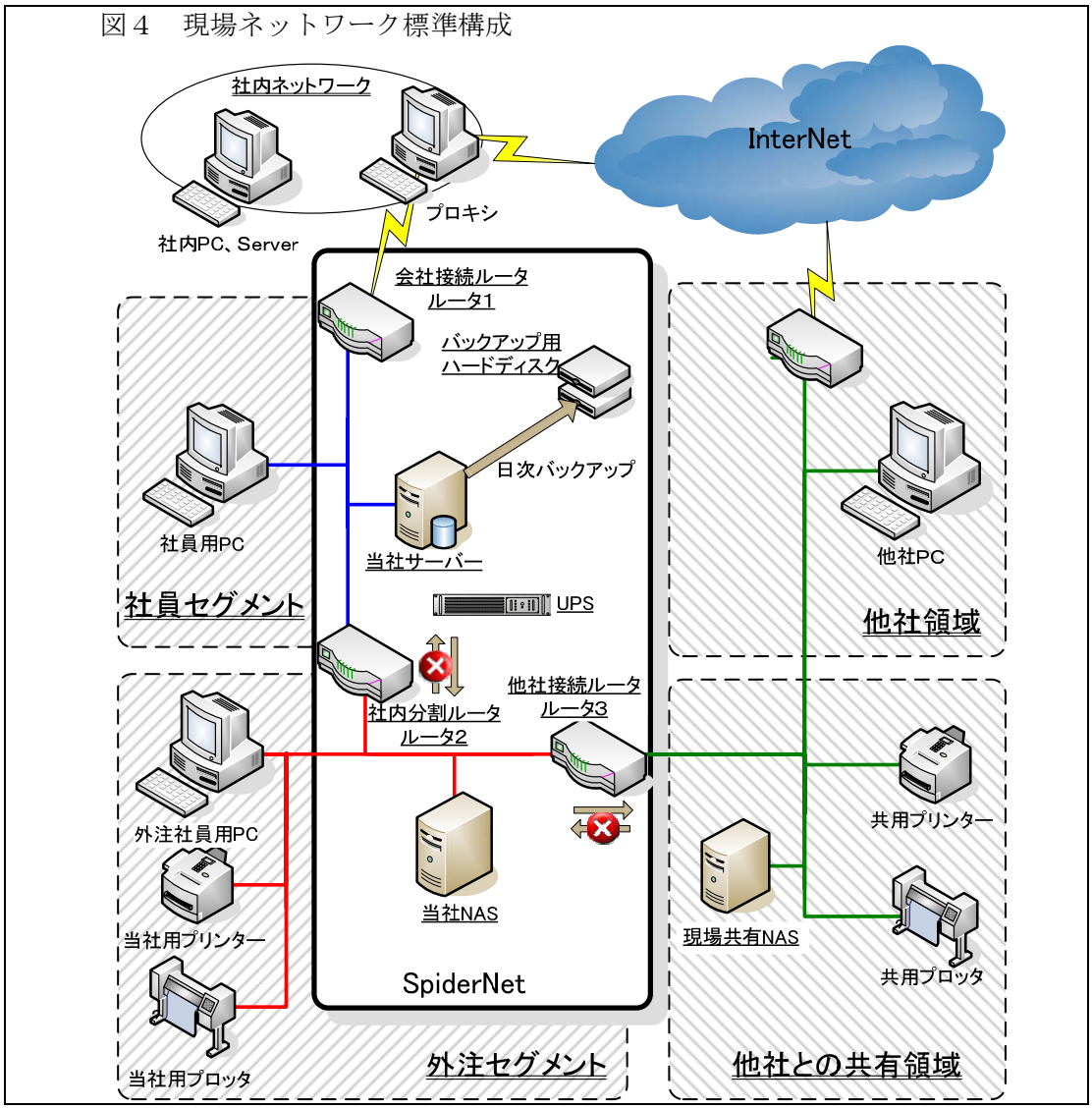
(5) 社内プロキシの代理プロキシ機能を搭載しセキュリティホールの発生を防ぐ.
(6) リモートディスクトップ機能を有効にし，本社からログインすることで，Q&A 対応や障害の切り分けなどのサポートや遠隔監視を行う.
(7) ローカルログオンは禁止とし，設定の変更や削除を防止する.
(8) 社員セグメントのみのデータ共有領域も提供する.
(9) 現場の電源の事情は劣悪なので，機器の保護の為に常時インバータ方式の無停電源装置を取り付ける.

3．3　現場ネットワーク標準構成

こうして考案されたネットワーク構成が図４である.

図４中央の太線で囲まれた機器類はどのような現場でも適用することが可能であり，これにより全現場のＩＴ環境の標準化が図れるようになる.

図４　現場ネットワーク標準構成



プロッタ，プリンタなどのリソースは他社との共有が必要であれば，他社との共有領域に接続するが，当社だけで利用する場合は外注セグメントに接続し，IP アドレスの標準化の対象とする.

現場での取り扱いを簡単にする為，太線で囲まれた部分の機器類を一体化させ組み付けたものを「SpiderNet」(Site Productivity Inspiring Developing and Enhancing Realization Network ： 現場生産性の鼓舞,発展,強化を実現するネットワーク)と命名した.

図５はSpiderNetの写真であり，表３は構成機器表である.

図５　SpiderNetの写真

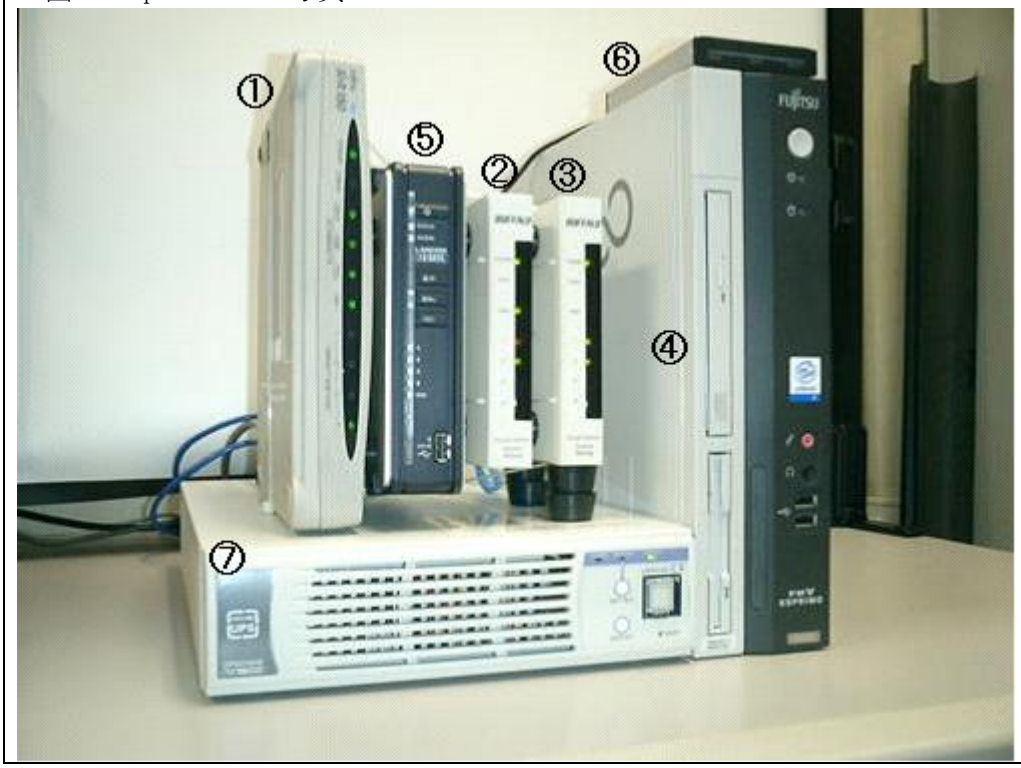


表３ SpiderNet構成機器表

写真の番号	構成機器名称	摘　　要
①	ルータ１	Si-Rシリーズ / ip-sec対応
②	ルータ２	ブロードバンドルータ
③	ルータ３	ブロードバンドルータ
④	当社サーバー	FMV ESPRIMO / WindowsXP
⑤	当社NAS	160GBの単機能のＮＡＳ
⑥	バックアップHDD	80GB のポータブル型 USB-ハードディスクを２台交互に利用する.
⑦	UPS	常時インバータ方式　350VA

３．４　社内申請，納品，設置完了までの流れの標準化

３．４．１　社内申請

SpiderNet の構成機器の中にルータ１（会社接続ルータ）があるが，これは既に現場に普及しており，接続用IDと共に既存のものを使用する場合が多い.

その為，導入時の手配は，接続用 ID，ルータ１，それ以外の機器，に別れるが，これらの社内申請を簡略化するため，ID と機器を全てデータベースに登録し，申請から納品，移設，廃棄までの管理を一元化した.

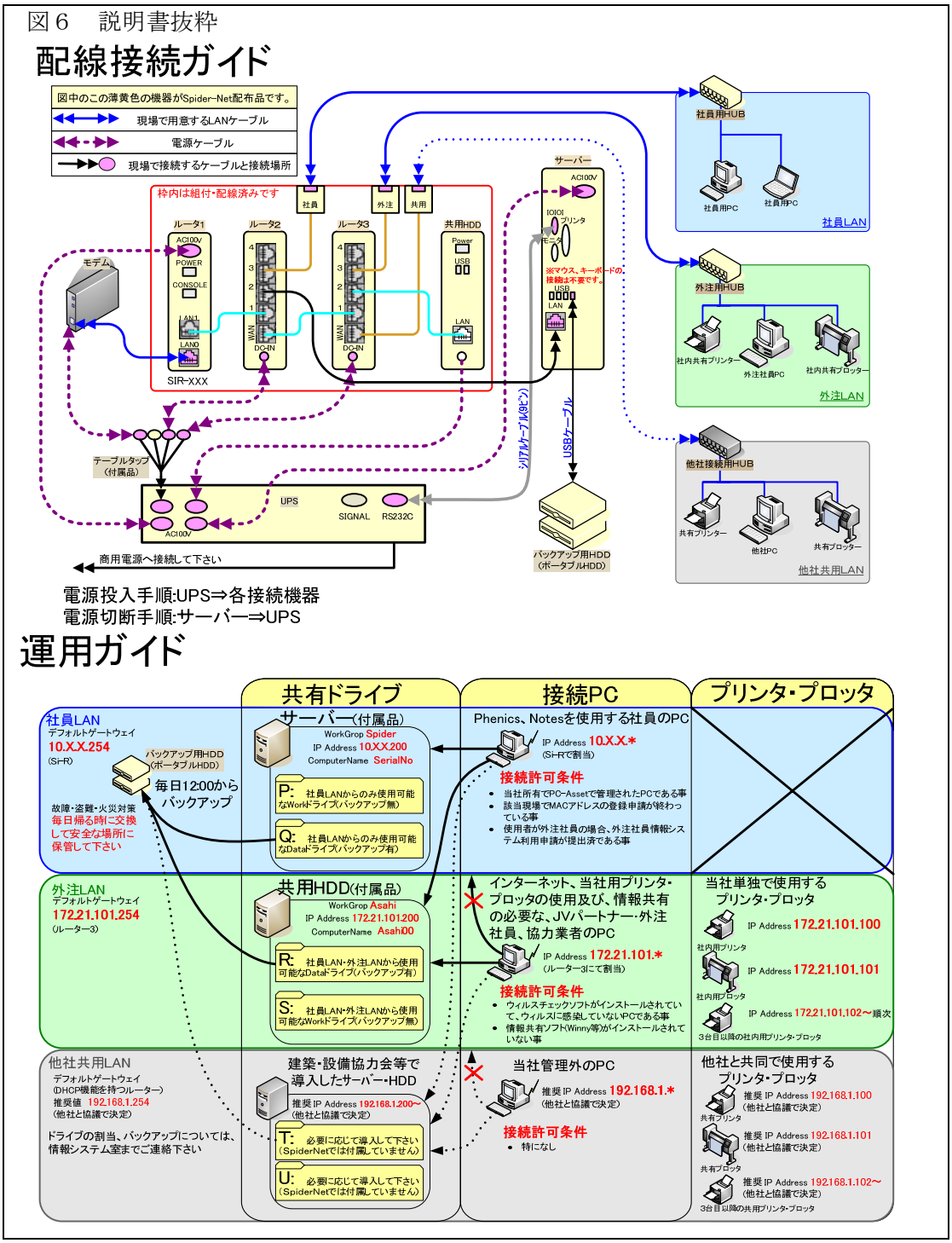
３．４．２　納品

SpiderNet の組付け，サーバーのインストール，ルータ等の設定は販売代理店に依頼した．速やかに納品する為，販売代理店の倉庫に在庫を持ち，必要時に現場固有の部分だけを設定して出荷できるようにし，依頼から５営業日後の納品を可能とした．

３．４．３　現場での設置

図６のような説明書を出荷時に同梱して，現場での設置，運用管理を簡易化した．

図６　説明書抜粋



４．導入効果の検証

４．１　導入状況

現在，テスト導入から一年，本格導入開始から半年経過し，導入実績は当社の現場の 15%程度となっている．

４．２　導入効果

SpiderNet は現場事務所の効率化要求を損なわずにセキュリティの向上を図ることを目的としているので，基本的な導入効果はセキュリティの向上と IT 環境の構築，運用の省力化であるが，今までスキル不足で環境を構築できなかった現場では２．１「現場事務所の効率化要求」で挙げた要求自体が効果となる．

主な効果は以下の通りである．

1. セキュリティの向上
   (1) 情報漏洩，ウイルス感染，不正侵入の阻止

   当社の領域(社員セグメント，外注セグメント)ではウイルスのバックドア活動， winny などの共有ソフトの活動を防止．

   共有セグメントからのネットワーク感染型のウイルスの侵入やウイルスの自己アップデートを防止．

   共有データの定期的なウイルスチェックの実施．

   (2) データの消失対策

   共有データの毎日の確実なバックアップによる下記リスクの低減．

   - HDD 故障時のデータ復旧費用　平均 30 万円/件
   - 火災，盗難などによるデータの完全消失時の被害額　平均 560 万円/件

2. IT 環境の構築，運用の省力化
   (1) ネットワーク構築時の省力化

   １現場平均２人日が0.5人日に軽減

   導入済みの９割以上の現場は設定変更なしで運用を行っている．

   (2) 迅速な障害対応の実現

   ネットワークなどの諸設定が全現場標準化されたことで，リソースの状態も本社から確認できるので，障害の切り分けやQ&A対応が速やかになり負荷が軽減された．

   未導入の現場では半日かかるような障害対応が導入済の現場では30分程度で終わる．

3. 現場事務所の効率化要求の実現
   (1) プリンタ等の他社との共有による経費節減

   1 現場平均 30,000 円/月

   (2) 情報共有スペース(ファイルサーバー)の提供による業務効率化

   1 現場平均２人日/月

   (3) 外注社員のインターネット接続による業務効率化

   1 現場平均３人日/月

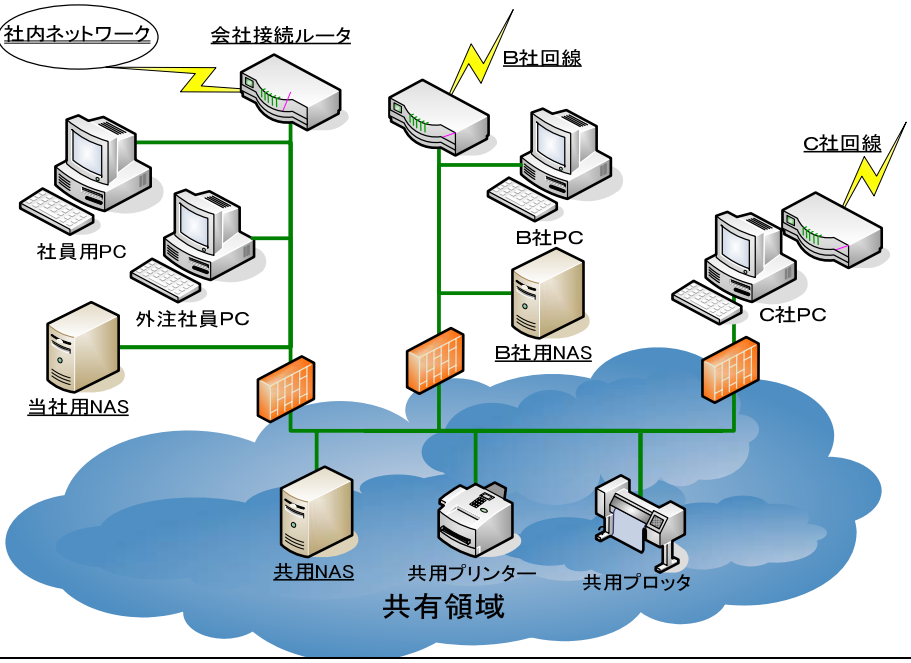
５．おわりに

内部統制強化により各社のセキュリティポリシーがますます厳しくなると，現場でのリソースの共有が難しくなる．

SpiderNet では，自社のセキュリティポリシーが及ばない共有領域は危険であるとの前提で，その接続はファイヤーウォール(図４のルータ３)を設けてリソースの共有を行っている．このように各社が自社のセキュリティポリシーでファイヤーウォールを設けると図７のモデルとなり，互いのセキュリティポリシーの影響を受けなくなる．

この考え方が建設業界全体に広まり，セキュリティポリシーの相違に阻害されずにリソースの共有化が進み，建設業全体の「セキュリティの向上」「業務の効率化」「コスト削減」が推進されれば幸いである．また，当社の取り組みをベースに更なる改良を加え，より良いものが考案されることを願うものである．

図７　現場ネットワーク構成モデル



最後にSpiderNetの現場への導入・運用の検討に際し，多大なご支援をいただいた株式会社富士通ビジネスシステム殿に感謝致します．