建設現場ネットワークの
構築と運用ガイドライン

2001年04月　初版

2024年02月　修正

一般社団法人 日本建設業連合会

建築生産委員会 ICT推進部会

情報セキュリティ専門部会

目　　次

1. はじめに

本ガイドラインは、建設現場ネットワークの安全・安定した運用と建設現場への容易な導入を目的に、2005 年 4 月発行の「JV 現場ネットワークの構築と運用ガイドライン(第 2 版)」、2008 年 11 月発行の「建設現場における情報セキュリティガイドライン(第 1 版)」との棲み分けを図って全面的に再編集した 2013 年 9 月発行の「建設現場ネットワークの構築と運用ガイドライン」、を現在の技術レベル、運用レベルに照らして見直して 2019 年 1 月に発行した第 2 版に一部更新をかけたものである。

今回の更新に際しては、利用が拡大しているメッセンジャーやオンラインストレージといったクラウドサービスの利用に関する記述を中心に追加した。

尚、ネットワークにおけるセキュリティリスクへの対応策については、現状の情報セキュリティリスクに対応できる最低限の対策を指針として記載しているため、本ガイドラインの内容に準拠していればリスク対策は万全、というものではない。個別のプロジェクト要件や新たに発生したセキュリティリスク等への対策については、関係者と協議・調整を十分に行ったうえで対応していただきたい。

1.1 ガイドラインの範囲

本ガイドラインは、建設現場のネットワーク構成とそこでのセキュリティの考え方、導入、維持管理方法、及びネットワークに関する費用の負担方法に関して、一般的技術を用いた実施しやすい方策や事例を示している。また、外部関係者及び構成会社本支店等との情報交換の手段として、サーバーを利用しての情報共有方法、建設現場からのインターネットへの接続方法、クラウドやスマートデバイスの利用・接続ルールなどについても示している。

尚、ネットワーク以外のセキュリティ対策については、「建設現場における情報セキュリティガイドライン(第 1 版)」を参照することとし、本ガイドラインの範囲外とする。

1.2 展開と取扱いについて

本ガイドラインは、建設業界の ICT 活用の方向性を示し、建設業界全体に広く利用を呼びかけるものとする。本ガイドラインの利用方法を、以下に挙げる。

(1) 社内標準作成の参考として

建設現場のネットワーク構築に関する社内標準が定められていない会社においては、社内標準作成の一助として利用できる。

(2) 外注システム業者への指示図書として

システムに関する業務を外部のシステム専門業者に委ねる必要が発生した場合、ネットワークの内容を的確に説明・指示できる資料として利用できる。

(3) JV 運営委員会・施工委員会でのひな形資料として

JV 現場のネットワーク構築計画において、運営方法を含めた合意事項のひな形として利用できる。

(4)協力会社の情報セキュリティ対策の強化を促す際には、要請の方法や内容が独占禁止法の優越的地位の濫用とならないように、「サプライチェーン全体のサイバーセキュリティ向上のための取引先とのパートナーシップ構築に向けて（令和 4 年 10 月 28 日経済産業省、公正取引委員会）(https://www.jftc.go.jp/dk/guideline/unyoukijun/cyber_security.html)」を遵守し、特に「第 3 取引先との関係構築」を留意すること。

2.　ネットワーク構成

(1) 構成方針

・ネットワークを介して関係者等の情報交換、及び共有が安全で円滑にできる。
・インターネット及び各社のイントラネットを利用できる。
・JV 現場の場合、関係各社は、各社毎のセキュリティポリシーを遵守できる構成とするが、各社の要件が相反する場合は、JV スポンサー会社のポリシーを優先する。

(2) 基本構成

・2.1 共通事項
　建設現場ネットワークの全体にかかわるものを解説し、ネットワークを構成する下記 3 項目について、それぞれに解説をしていく。
・2.2　現場事務所内ネットワーク
　各自の利用するパソコンやサーバーやプリンターなどの共有資源とネットワーク機器で構成されており、それらのセキュリティ設定や留意点について解説する。
・2.3　企業内ネットワーク及びインターネットへの接続
　現場事務所内ネットワークから各社のイントラネットやインターネットに接続するための通信方法や通信機器についてのセキュリティ設定や留意点について解説する。また、モバイル通信サービスの利用者、JV 現場における回線の共有方法についても解説する。
・2.4　施工現場でのネットワーク
　事務所から離れた施工現場で、スマートフォンやタブレット等のモバイル機器・WEB カメラ・計測機器などの情報機器利用のためのネットワーク構築や、現場事務所内ネットワークとの接続方法について解説する。

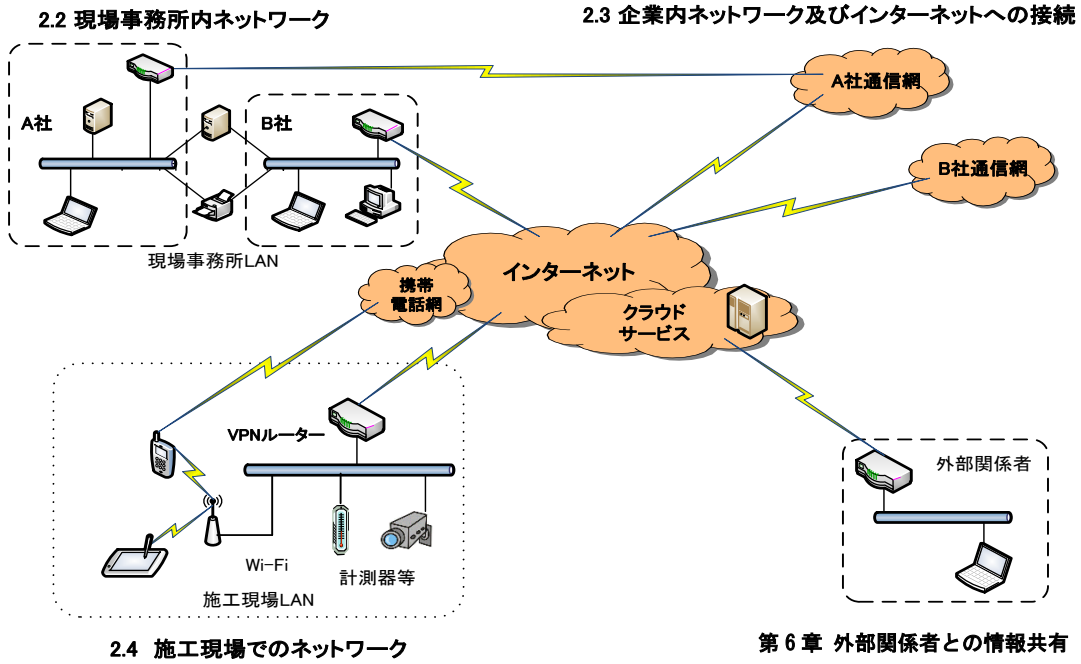

図 2-1　建設現場ネットワーク例

2.1 共通事項

(1)LAN 方式

有線 LAN、無線 LAN は、それぞれの特性を生かし適材適所で利用する。ただし、無線 LAN は、セキュリティ対策と運用管理を適切に行うことを利用の条件とする。セキュリティ対策については「4.3 無線 LAN 利用時の対策」を参照のこと。

(2)通信プロトコル

通信プロトコルは、TCP/IP を標準とする。JV 現場にて、TCP/IP 以外を使用する必要がある場合には、JV 構成会社間で協議する。

(3)ネットワークセグメント

JV 構成会社毎にネットワークセグメントを分けた複数セグメントを基本とする。1 セグメントでは、JV 他社パソコンの共有フォルダ（スキャンしたドキュメントの保存先等）やアクセス権設定の甘いサーバーにアクセスできるなどセキュリティリスクが高くなる。ただし、小規模な構成の場合など、セキュリティのリスクを受容できる場合は１セグメントの構成も可とする。

表 2-1　1 セグメントと複数セグメントとの比較

	メリット	デメリット
複数セグメント	・セグメント間で通信制御が可能であり、セキュリティを確保しやすい ・ウイルス発生時の拡散防止や障害時の問題箇所の特定が容易	・構成が複雑になるため、設計や構築に際して専門知識が必要 ・情報共有するための設計が複雑
2 セグメント（複数セグメントの簡易版）	・JV スポンサー会社とそれ以外の JV 構成会社の 2 セグメントに分ける場合は、サーバーや複合機の通信カードを 2 枚用意すれば済むため、構成が簡素で JV スポンサー会社のセキュリティ確保が容易	・スポンサー以外の JV 構成会社が 2 社以上になった場合は JV 構成会社間のセキュリティ確保が困難
1 セグメント	・構成が簡素なため、構築や維持管理が容易 ・情報共有が容易	・セグメント内での通信制御が困難であり、セキュリティを求められる現場には向かない ・ウイルス発生時の拡散防止や障害時の問題箇所の特定が困難

(4)アクセス回線

単独の場合は問題にならないが、JV 現場においては、JV 構成会社やインターネットへのアクセスに用いる回線の種類は各社各様であるため、JV 構成会社ごとにアクセス回線を準備する。ただし、JV 構成会社間の協議にてアクセス回線の共有を取り決めた場合はこの限りではない。

また、アクセス回線を敷設する前に、取り扱いデータを事前算定し、ネットワーク負荷を評価する。評価結果によって、回線種別の見直しや個別単位での専用ネットワークの敷設を検討することが望ましい。

表 2-2　回線種別と通信速度

種別	通信速度（理論値：最大）
光回線	100Mbps～1Gbps
携帯電話回線	37.5Mbps～150Mbps
ADSL	1.5 Mbps～47Mbps（下り）
ISDN	64kbps～128kbps

(5) インターネットへの接続

建設現場ネットワークからインターネットを利用する場合は、各企業内ネットワークを経由することでセキュリティを確保することを基本とするが、セキュリティを考慮した上で建設現場ネットワークからインターネットへの直接接続も可能とする。

インターネットに直接接続する場合、セキュリティ企業の 2019 年度報告では、インターネット上で保護されずに誰でもアクセス可能な状況にあるファイルの総数が 23 億に達しており、また、パソコンやサーバーをネットワークに接続すると1分未満でサイバー攻撃の標的になることが実証されている。

インターネットへの接続はそれほど危険なものであるということを認識して、相応の対策をとらなければならない。　詳細は 2.3 (2) を参照のこと。

(6)モバイル通信サービスの利用

短工期現場、現場事務所開設前の仮事務所、リニューアル・改修工事等で有線設備を設けることができない場合や、回線開通までの一時利用の場合には、モバイル通信サービスが利用できる。

(7)JV 構成会社への接続

JV 現場ネットワークと各 JV 構成会社の企業内ネットワークとの接続においては、ルーターに備わっているフィルタリング機能等を使って、それぞれの構成会社の企業内ネットワークに、自社の職員だけが接続できるように制限する。

(8)協力会社、設計事務所等の接続

協力会社等のパソコンは、建設現場ネットワークに接続しないことを基本とする。ただし、その必要がある場合は、「(7)JV 構成会社への接続」に準ずる。

(9)タブレット端末、スマートフォン（以降スマートデバイス）

スマートデバイスは、各企業のセキュリティポリシーに従って利用する。JV 現場においては、構成会社で協議する。

(10) 外部関係者との情報共有

建設現場ネットワーク外の発注者や協力会社等の外部関係者との情報共有を求められる場合は、外部のサービス（クラウド等）を利用することを基本とする。建設現場ネットワーク内のサーバーを外部関係者からアクセス可能にすることはセキュリティを低下させるため、禁止する。

クラウドサービスの利用にあたってのセキュリティ上の事前評価や運用体制に関する注意事項は、第６章 外部関係者との情報共有（クラウドサービスの利用）を参照のこと。

2.2　現場事務所内ネットワーク

(1) IP アドレス

①プライベートアドレスのクラス C を採用する

ネットワークに接続するパソコンやルーター・サーバー等の機器の合計が 254 台以下であれば、クラス C（192.168.m.n）の IP アドレスを使用し、1 セグメント m＝0～255 のうち任意の 1 つを利用し（1 を利用することが多い）、各端末は n＝1～254 のうち任意の 1 つを利用する。

また、パソコンや接続機器の増加による IP アドレスの不足、及び、より強固なセキュリティの要請などで複数セグメントにする場合は、それぞれのセグメントに異なるクラス C（m＝0～255 を重複させない）を割当て、ルーター等を用いて接続するなど別途構成を検討する。

②JV 構成会社の IP アドレス体系と整合をとる

各構成会社に接続する際には、その接続を行うルーターの持つ IP アドレス変換機能（NAT 機能）により各社の IP アドレス体系との整合をとる。これにより、どの JV 現場にも同じアドレス体系を用いることができる。

③JV 現場の場合に推奨する IP アドレス配布方法

各 JV 構成会社に「10」単位ずつ配布することで、各構成会社との接続の構築作業と IP アドレス管理の簡素化が図れる。採番方式及び IP アドレス採番例については、「5. JV 現場ネットワークの構築手順と事例」を参照のこと。

④JV 現場の場合に推奨する動的な IP アドレスの付与（DHCP 機能の利用）について

1 セグメントにつき 1 社のみ DHCP 機能を利用可能とし、これ以外は静的に IP アドレスを付与していく。ただし、DHCP 機能が何らかのネットワーク障害を誘発する場合は、直ちに DHCP 機能を停止する。

(2)共有サーバー

建設現場ネットワークにおける円滑な情報共有方法として、共有サーバーや NAS（Network Attached Storage）を設置することが一般的である。しかし、共有サーバーの利用においては、いろいろなパソコンが接続された状態で、悪意を持った利用者により、サーバーのデータを自由に閲覧できたり、改ざんされたりする恐れがある。また、昨今の情報漏洩問題や、ウイルスによる感染など、今まで以上に注意を払う必要がある。

①共有サーバーの設置場所

・現場事務所内（複数セグメントの場合）

共有サーバーは、複数あるセグメントのうち、共通のセグメントに設置する。また、可能であれば、不正操作を防ぐため、鍵のかかる小型のサーバーラック等に収納する。

・現場事務所内（2 セグメントの場合）

共有サーバーは、通信カードを 2 枚用意し、2 つあるセグメントそれぞれに接続できる場所に設置する。

・現場事務所内（１セグメントの場合）

共有サーバーは、現場事務所内のセグメント上に設置し、可能であれば、不正操作を防ぐため、鍵のかかる小型のサーバーラック等に収納する。

・外部（クラウドサービス〈インターネットストレージサービスや ASP など〉を使う場合）

共有サーバーは、クラウド上（インターネット上）に置かれる。その場合、設置しているデータセンターの管理は適正か、適切なセキュリティ設定がされているかを確認する。

なお、詳細については、「6　外部関係者との情報共有（クラウドサービスの利用）」を参照のこと。

②データのセキュリティ設定

不正なアクセスを防ぐため、共有サーバーへの接続はユーザーID・パスワードで認証し、共有されるデータ（フォルダーやファイル）には適切なアクセス権を設定する。

なお、詳細については、「4.4　共有サーバー（NAS）利用時の対策」を参照のこと。

③安全性の確認

本ガイドラインでは、共有サーバーを外部からアクセスできるようにすることは基本的には禁止しているが、セキュリティを考慮した上での建設現場ネットワークからインターネットへの直接接続は可能としている。その場合、意図せず誤った設定になっていることも考えられるので、以下のような情報を参照して安全であることを確認する必要がある。

IPA 独立行政法人 情報処理推進機構
「増加するインターネット接続機器の不適切な情報公開とその対策」
https://www.ipa.go.jp/about/technicalwatch/20140227.html

(3) プリンター・複合機

最近のプリンターや複合機は、ほとんどがネットワーク接続に対応している。設定も簡単なため、ネットワーク対応のプリンターや複合機を導入する。

プリンターや複合機を構成会社で共有する場合は、共有セグメントに配置する。

(4) ネットワーク構築における留意事項

①スイッチングハブ等のポート数は、人員の増減を見越して設定する。ポート使用率は、急な利用増を見越して7割程度にして、残りはリザーブしておくとよい。空きポートに不正な機器が接続されないよう注意する。不正接続や不正抜去を防ぐ製品を利用することも効果がある。

②LAN ケーブルは、不正利用を避けるため必要最小限にとどめる。利用していない LAN ケーブルは、撤去する。

③複数セグメントを採用した場合は、セグメントごとに LAN ケーブルの色を変えるとよい。

④ネットワーク構成図を作成し、構成の変更時にはメンテナンスする。

⑤ネットワーク機器は、金具などで固定しておくとよい。

2.3 企業内ネットワーク及びインターネットへの接続

(1) 建設現場から企業内ネットワークへの接続

建設現場から企業内ネットワークに接続するには、現場側にアクセス回線及びルーターを用意し、ルーターのフィルタリング機能を使って不必要な通信を制限する。

また、インターネット回線は盗聴等のリスクがあるため、企業内ネットワークへの接続では VPN（バーチャル・プライベート・ネットワーク）を利用する。VPN には以下のものがあるが各企業内で定められた方法を用いる。

①IP-VPN ：通信キャリアーが提供する VPN サービス

②インターネット VPN：インターネットを利用した VPN 接続

・LAN 型 VPN ― LAN 同士を専用ルーター等で接続する

・リモート型 VPN ― パソコン等からブラウザまたは専用クライアントを用いて接続する

IPsecVPN：パソコン等に専用のクライアントソフトを組み込む

SSL-VPN：主にブラウザ等を経由する

JV 現場の場合、各構成会社はアクセス回線及びルーターを用意し、ルーターのフィルタリング機能を使って自社の職員だけが各企業内ネットワークへ接続できるように制限する。

ルーターの設定変更や自社開発アプリケーションのメンテナンス等のために、JV 現場外（たとえば JV 構成会社の企業内ネットワーク）から JV 現場内ネットワーク上の機器にリモート接続する場合は、あらかじめ各 JV 構成会社との協議又は報告を行った後、接続する。さらに不正アクセス及び不必要な通信を防ぐための接続制限等のセキュリティ対策を行う。

(2)インターネットへの接続

建設現場からインターネットへの接続は、ファイアーウォールの設置やスパムメール、ウイルスへの対応がされている各企業内ネットワークを経由することでセキュリティを確保する。企業内ネットワークを経由せずに直接インターネットへ接続する場合は、それにより生じる以下のセキュリティリスクを十分に理解するとともに必要な対策を講じる。

① コンピューターウイルスの感染

②インターネットから建設現場内ネットワークへの不正アクセス

③建設現場内ネットワーク上のサーバーやパソコンなどの不正使用（乗っ取り、踏み台等）

④建設現場内ネットワークの盗聴、サーバーやパソコンなどのデータ改ざん、破壊

対策例

① IP マスカレード等による建設現場内ネットワーク内の IP アドレスの隠ぺい

② インターネット接続できるパソコンをルーターに登録（IP アドレスなど）

③ ルーターの管理用パスワードの管理と定期的変更

④ インターネットからルーターへの直接接続（telnet 等）やサービス要求を拒否

⑤パケットのフィルタリング

例）Windows のファイル共有、IP アドレスの成りすまし、ルーターに対する ping などのフィルタリング

⑥ルーターのファームウェアの適時更新

⑦外部から不正にアクセスされない設定と、その設定が間違いないことの確認
・ペネトレーション（侵入）テスト／監査
・設定に問題がないことの確認
参考：IPA「増加するインターネット接続機器の不適切な情報公開とその対策」
https://www.ipa.go.jp/about/technicalwatch/20140227.html

(3)モバイル通信サービスでの企業内ネットワーク接続
モバイル通信サービスとしては以下のものがある。
①携帯キャリアーの提供するモバイルルーター若しくはスマートフォンのテザリング
ルーター及びスマートフォンからインターネットへの接続は携帯キャリアーの通信回線（LTE・3G）を利用し、ルーター及びスマートフォンとパソコンとの間は無線 LAN の機能で接続する方法。少人数で共有可能（通常同時接続機器 5～10 台まで）
②携帯キャリアーの提供するデータ通信カード（主に USB 接続）利用
データ通信カードを直接パソコンに接続し、携帯キャリアーのプロバイダー経由でインターネットに接続する方法。基本的にパソコン１台につき１つのカード利用が主だが、Windows のインターネット接続の共有機能を使うことで LAN 内の他のパソコンと通信を共有することができる。
モバイル通信サービスで企業内ネットワークに接続する場合でも企業内で定められた VPN を使用する。ただし、VPN の方式によっては、利用できる機器に制限があるので注意が必要である。また、自社で許可されている場合でも、JV 現場においては各構成会社と協議の上、利用の可否を判断する。

(4)JV 現場における回線の共有
前述のとおり、JV 現場においては構成会社毎にアクセス回線を用意することを原則とするが、構成会社間で合意された場合にアクセス回線を共有することができる。
（アクセス回線の共有事例）
通信事業者のサービスによっては、1 本の物理回線（ADSL 等）で複数のセッションが利用（複数の ISP に接続）できる。ただし、この方式で回線を共有する場合は、終端装置と直接ルーターを接続することを前提にしたサービスもあるため、事前に通信事業者へ確認する必要がある。
回線共有時のセキュリティ対策については「4.2 回線共有利用時の対策」を参照のこと。

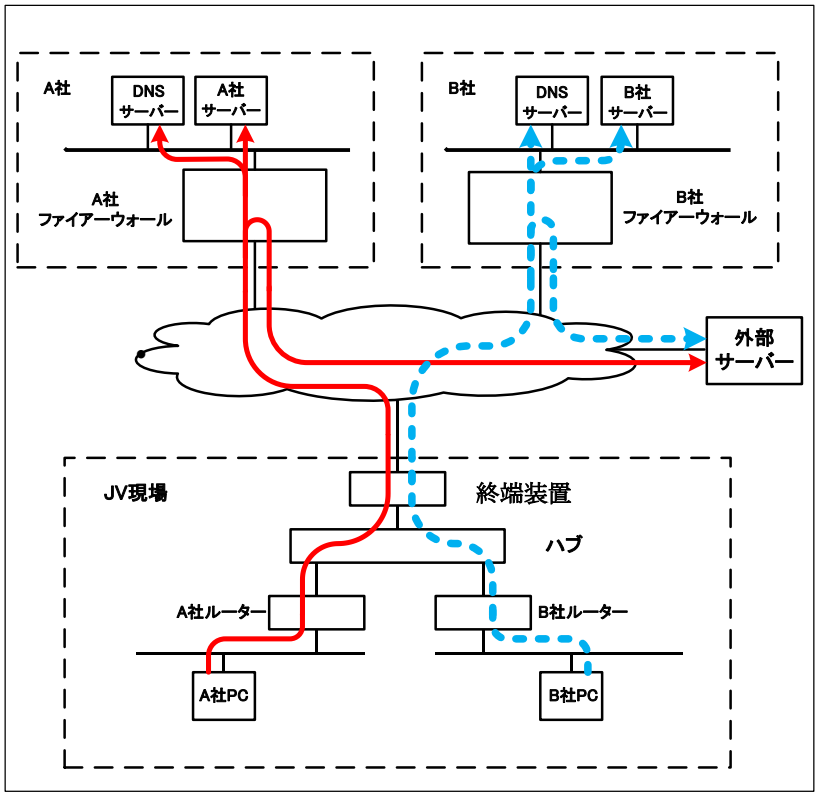

図 2-2　JV 現場における回線共有時の通信経路

2.4　施工現場でのネットワーク

建設現場での情報機器利用については、現場事務所内での利用のみならず、実際の施工現場においてスマートフォンやタブレット等のモバイル機器が利用されるようになってきた。

ここでは、建設現場ネットワークを現場事務所ネットワークと施工現場ネットワークとに分け、施工現場での情報機器利用のためのネットワーク構築について述べる。

(1)施工現場と現場事務所とのネットワーク接続方法

施工現場の各種計測機器や監視カメラなどの情報をリアルタイムに把握するため、施工現場で職員が情報機器を利用して現場管理を行うケースが増えてきている。一方、施工現場のネットワークには、発注者や協力業者等の PC・スマートフォンやタブレット端末等のモバイル機器の接続も予想されるため、施工現場 LAN と現場事務所 LAN との接続は、VLAN などで独立させることが望ましく、施工現場内で使用する機器に関しては、計測機器等は固定 IP を割り当て、Wi-Fi などによる接続機器に関しては、MAC アドレス認証等によりセキュリティを高めた接続が望ましい。また、施工現場での Wi-Fi 利用・スマートデバイス利用に関しては、「4.3 無線 LAN 利用時の対策」・「4.5 スマートデバイス利用時の対策」を参照のこと。

①ケーブルの延長による接続

現場事務所 LAN を延長した形での接続である。施工現場の LAN との接続には、通常 LAN ケーブルが用いられるが、距離が離れている場合などは、マイクロ波による無線接続などが用いられることもある。

図 2-3　ケーブルの延長による接続

②通信キャリアーが提供する通信回線経由での接続

施工現場と事務所が遠距離で、有線接続を行う場合、通信キャリアーの VPN サービスを利用して接続することが可能である。この場合、自社ネットワークとの接続も可能である。

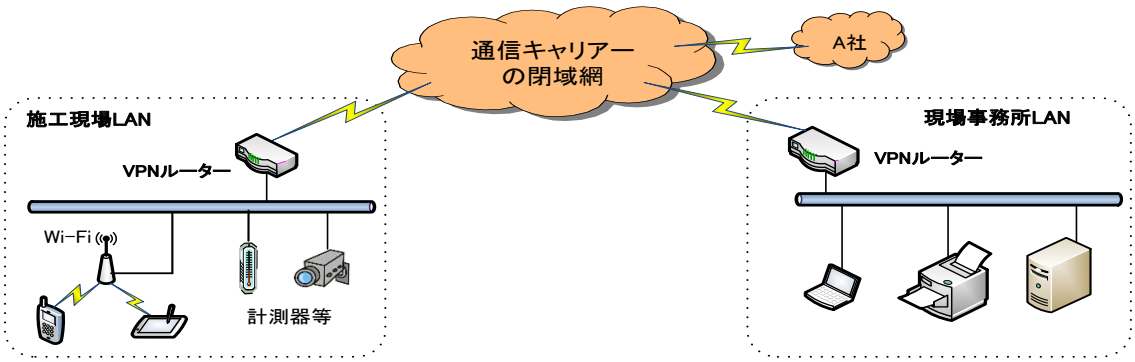

図 2-4　通信キャリアーの VPN サービスを使った接続

③インターネットを利用した接続

VPN サービスを利用せず、直接インターネットを利用して事務所の LAN と接続するには、SSL-VPN やインターネット VPN でセキュリティを確保する。外部公開されている計測機器や Web カメラを制御・利用する必要がある場合は、基本的に各社の方針に従った範囲での利用に限り、各社の情報管理者の指示のもとセキュリティを確保できる状態で利用する。

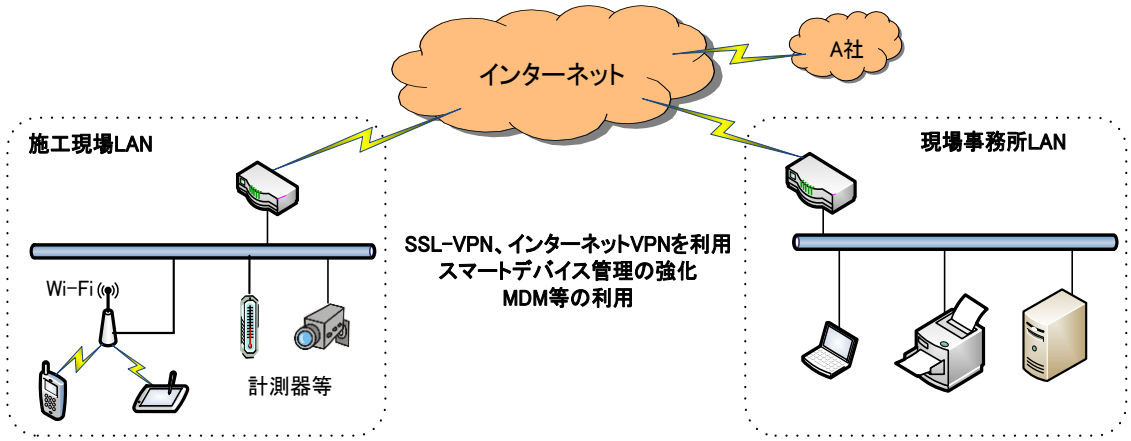

図 2-5　インターネットを利用した接続

(2) 施工現場や現場事務所でのスマートデバイスの接続

①スマートデバイスと現場事務所 LAN との接続

施工現場や現場事務所でのスマートデバイスの接続については、施工現場のネットワークに Wi-Fi アクセスポイントを設置する方法と、通信キャリアーの回線網を利用する方法とがある。

スマートデバイスは、MDM を導入し、リモートロック・リモートワイプ・機能制限等によるセキュリティの強化が必要である。実施に関しては、各社のスマートデバイスの運用方針に従った上で使用する。

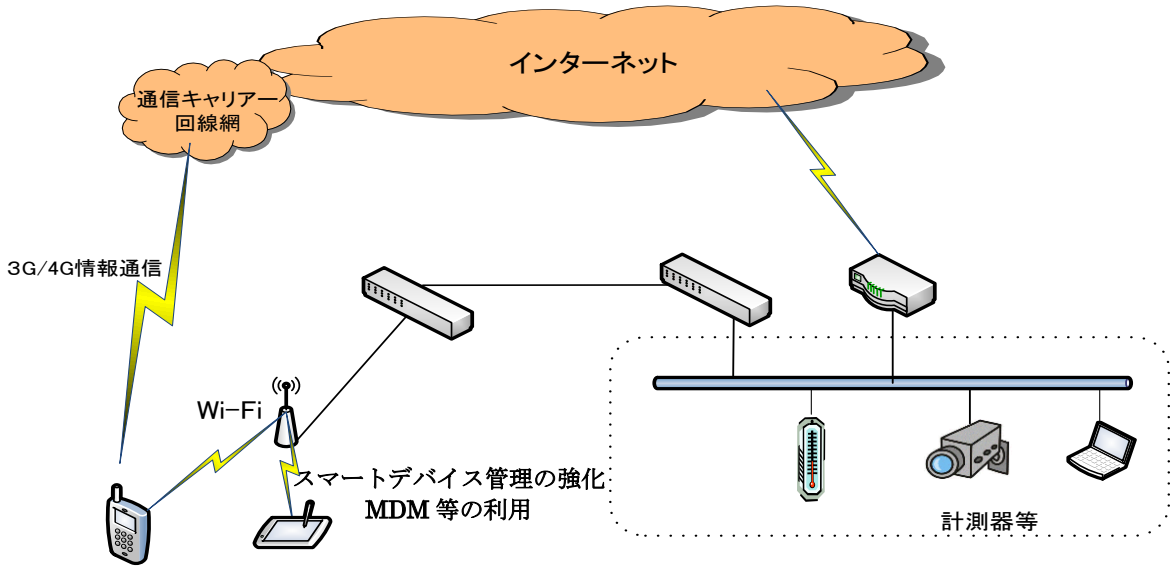

図 2-6　スマートデバイスを利用した施工現場 LAN

②スマートデバイスによる施工現場の直接監視

施工現場と現場事務所は接続せず、各種計測機器や監視カメラの情報をスマートフォンやタブレットで直接監視するケースが今後増えてくると予想される。

監視の方法としては、Wi-Fi 等を利用して現場内でクローズした利用が望ましいが、発注者等の利用など外部からの監視が必要な場合は、モバイル通信サービスを利用し、インターネットからの接続が要求される。この場合、計測機器や監視カメラが直接インターネットに晒されているため、盗聴やなりすまし等のリスクがある。ユーザー認証やパスワードの定期的な変更等、セキュリティ対策（「4.5 スマートデバイス利用時の対策」を参照）をとることが望ましい。

3. ネットワーク維持管理

建設現場ネットワーク構築後の運営段階においては、ネットワークアドレス表の整備などの日常管理や、ネットワーク障害復旧を行う体制が必須となる。これら維持管理作業を円滑に行うため、現場内に「ネットワーク担当者」を定める。JV現場の場合は、会社毎にネットワーク担当者を定め、JV 幹事会社のネットワーク担当者が構成会社のネットワーク担当者を取りまとめ、JV 発足時のネットワーク構築作業からその後の維持管理作業を行う。

3.1 ネットワーク担当者の選任

構成会社のネットワーク担当者については、JV現場内から人選するのが好ましいが、構成会社の情報システム部門又は関係部門の担当者を選任してもよい。

表 3-1 JV 現場の各社ネットワーク担当一覧の例

構成会社	氏名	所属	電話番号	連絡先（電子メール）	備考
幹事会社Ａ	建 設 太郎			kentaro@aaa.co.jp	作業所内担当者
	建 工 次郎	情報システム部	xx-xxxx-xxxx	kenjiro@it.aaa.co.jp	本店情シ担当
構成会社Ｂ	土 木 太郎			doboku@bbb.co.jp	
構成会社Ｃ	建 築 次郎			kennji@ccc.co.jp	

3.2 ネットワーク担当者の役割

(1)機器、ネットワーク回線、ソフトウェア管理

現場ネットワークで利用するサーバーやルーター、ネットワーク回線、プリンター、パソコンなどの機器、ソフトウェアについて、導入手配及び障害時の連絡窓口となる。構成会社のネットワーク担当者は、新規に機器をネットワークに接続する場合は、必ず幹事会社のネットワーク担当者に申請する。

(2)ネットワーク（IP）アドレス管理

IP アドレスを管理するにあたっては、付与したIPアドレス、パソコン（機種／コンピューター名）等の機器名、それらの所属又は使用者を文書化しておく。また、機器の追加など必要に応じてIPアドレスの割当てを行う。JV現場の場合は、幹事会社のネットワーク担当者が、構成会社へのIP アドレスの割当てを行う。

(3)ネットワーク障害対応

現場内でネットワークトラブルが発生した場合に障害の連絡窓口となり、何処に連絡するかを判断する。JV現場において構成会社が導入したパソコン、通信機器、ネットワーク回線、ソフトウェア等の障害は、構成会社のネットワーク担当者が対応する。また、JV 現場内への影響が想定されるネットワーク障害が発生した場合は、幹事会社のネットワーク担当者に連絡する。

(4)セキュリティ管理

「建設現場における情報セキュリティガイドライン」に記述されている各種セキュリティ対策を実施する。JV現場の場合は、幹事会社のネットワーク担当者の指示に従って、構成会社のネットワーク担当者が各種セキュリティ対策を実施する。

(5)インターネットサービスの連絡窓口

現場独自に締結するプロバイダー契約やアウトソース契約の運用担当者となり、ユーザーID 管理や障害時の復旧窓口となる。JV現場の場合は、幹事会社のネットワーク担当者が担当する。

(6)各種管理資料の維持

上記(1)～(5)に係わる各種管理資料の策定、維持管理を行う。(付録-1参照)

3.3 JV 現場における考慮事項

(1)費用負担

パソコン、ネットワーク及びその関連機器などの導入費用、また、通信費、保守費、障害対応などの運用費用については、構成会社の自社接続費用も含め、共通原価で負担するのが望ましい。ただし、構成会社の自社接続費用等を共通原価として扱うためには、自社のパソコン使用料や通信回線費用の構成をJV構成会社に開示して合意を受けなければならない。また、JV に寄与しない構成会社独自のソフトウェア(自社開発ソフトウェアや自社購入ソフトウェア)等の費用は、構成会社それぞれが単独経費で負担すべきである。JV における費用負担項目は、最終的にはJV 運営委員会で取り決めるものとする。

費用を構成する項目としては下記のものがある。

表 3-2 費用を構成する項目 (例)

項目		項目	
ハード	パソコン、モニター	通信	LAN 配線
	ルーター		通信回線料金
	無線 LAN 機器		通信設定工事
	サーバー (NAS)	サービス	機器保守
	プリンター		プロバイダー契約料
	プロッター		ASP 料金
ソフト	JV 現場共通ソフト		電子商取引サービス料
	構成会社独自ソフト		

(2)周辺機器の管理と障害時の対応

周辺機器の管理と障害時の対応は、その機器を資産とする構成会社が行うことを原則とし(JV 共有で利用する機器は幹事会社のネットワーク担当者が対応を行う)、情報機器やソフトウェア等の導入は、構成会社の導入手続きにより実施する。

4. セキュリティ対策

4.1 LAN 共有時の対策

現場事務所内においてはＪＶ構成会社だけではなく、設計事務所・協力会社等の外部関係者との情報共有や複合機等の機器共有が必要になる場合がある。各社のネットワークを独立させるのが基本であるが、その際には、関係者への情報漏洩や関係者によるデータ破壊等のリスクに対して対策をする必要がある。また、このようなネットワークを安全に構築・維持していくためにはネットワーク管理者を設ける必要がある。

(1)ネットワークの構成

LAN を物理的に共有する場合には、各社毎に VLAN で LAN セグメントを分割し、情報共有サーバーや共用機器は各社からアクセスが可能な共有のセグメントとする。その際は、各社セグメント、共有セグメント間の通信は適切にアクセス制御を設定する。また、情報共有や共用機器が不要な場合や高度なセキュリティが求められる場合は、LAN を独立させる。

(2)情報共有サーバーの配置

情報共有サーバーは共有セグメントに配置し、ネットワーク管理者は利用するユーザー毎に適切なアクセス権を設定する。情報共有サーバーの利用時の対策については「4.4　共有サーバー（NAS）利用時の対策」を参照のこと。

(3)複合機等の共用機器の配置

共用機器は共有セグメントに配置する。

(4)対策例

ネットワーク管理者は、VLAN を構築、運用する場合は以下の対策を講じる。

①管理用 ID のパスワードは、初期値から変更する。
②スイッチングハブ本体にポートのグループ別に色分けした図等を貼付する。
③接続するパソコンには指定された IP アドレスを設定してから､スイッチングハブの指定されたポートに接続する。
④可能であれば、セグメント別に LAN ケーブルの色を変える。
⑤ネットワーク完成図書には、設定情報として IP アドレス、VLAN グループの名称、ポートの割り当て状況、グループ間のアクセス制御などを含める。

4.2 回線共有利用時の対策

現場事務所におけるアクセス回線は、JV 構成会社各社仕様の違いなどがあるため、JV 構成会社ごとにアクセス回線を準備することを基本とする。しかし、JV 構成会社間の協議により、アクセス回線共有の合意が形成された場合はこの限りではない。その際の主な特徴とセキュリティ上の対策例を以下に示す。(アクセス回線にも、ブロードバンド（FTTH、ADSL 等)、イーサネット、専用回線などがあるが、現在一般的となっているブロードバンドを例に記述する。)

(1)複数の接続が設定可能

光回線若しくは ADSL 回線において、1 つの回線契約で複数の接続先（プロバイダー）に同時接続ができる。標準で 2 セッションまでの契約が主流となっているが、追加契約により、上限(5～20 セッション）まで増加できる。

(2)回線共有の構成

ONU（終端装置）からハブで分岐して接続する方法と、マルチセッション対応ルーターを使う方法の 2 つある。(図 4-1 参照)

マルチセッション対応ルーターを利用する場合は、各社のプロバイダーの情報がお互いに確認できてしまうため、漏らさないよう注意する。

①ONU（終端装置）からハブで分岐して接続する方法

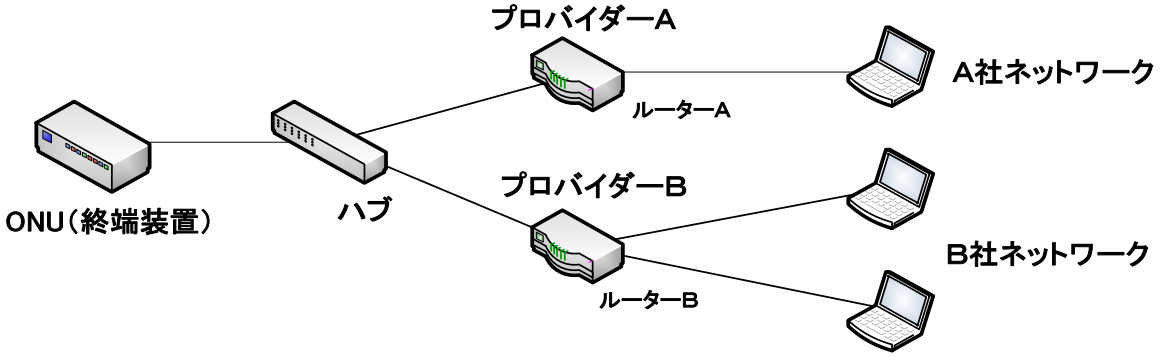

図 4-1　回線共有の構成 1

②マルチセッション対応ルーターを使う方法

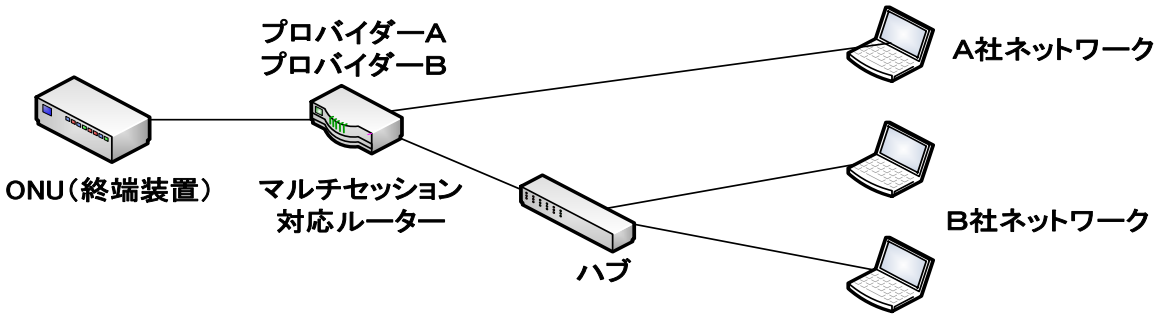

図 4-2　回線共有の構成 2

(3)セキュリティ上の対策例

①ルーターに設定するそれぞれのプロバイダーの ID、PW は厳重に管理する。

②トラブル発生時に問題を切り分けする観点から、スイッチング HUB で分岐する方法を推奨する。

③インターネットへの接続は各社ネットワークを経由することを基本としているが、直接インターネットへ接続するケースの場合は、各種セキュリティ機能を検討する。

・ルーター関連のセキュリティ機能

NAT 変換機能、動的なパケットフィルタリング　等

・プロバイダーが提供する各種セキュリティサービス

不正サイト制限、ウイルス感染防止、P2P フィルター　等

④ネットワーク管理者は、ネットワークデータ量と契約する帯域等を考慮して、レスポンス等の品質（可用性）についても十分かどうか監視する。

4.3　無線 LAN 利用時の対策

近年、無線 LAN は、手軽さ、利便性から家庭でも普及が進むとともに、新しい情報機器であるスマートデバイスにも標準装備されていることから、現場事務所への導入要望は根強いものがある。しかし、無線 LAN は、LAN ケーブルの代わりに電波を利用してデータを送受信するため、構築時のセキュリティ対策や利用者の登録/変更管理等の運用を適切に行わないと情報漏洩のリスクが高くなる。

以下に運用上の注意事項・対策例をあげる。

(1)ネットワーク関係者の承諾

一部でも無線 LAN を導入する場合は、以下のような影響を与える可能性があるため、ネットワークの関係者（JV 構成会社、協力会社、設計監理会社等）に承諾を得る。

①施主との情報セキュリティに関する契約事項に抵触

②無線 LAN 親機（アクセスポイント： AP）に設定する IP アドレスの重複による障害

③モバイルルーターとの干渉

(2)AP のセキュリティ設定

なりすまし、盗聴、不正利用、不正アクセス等のセキュリティ上のリスクを低減するため、AP に対し以下のセキュリティ設定を行う。

①ネットワーク認証、通信データの暗号化
②セキュリティ規定等で定められた文字種類、桁数を満たすネットワークキー（暗号化キー）
③セキュリティ規定等で定められた SSID（又は ESSID）の命名、「Any 接続拒否」及び「ステルス機能」の有効化
④クライアント（子機）の認証（MAC アドレス認証又はクライアント証明書）

(3)無線 LAN 設定情報の管理者の選任

以下については、無線 LAN のセキュリティを確保するための機密情報であるため、この情報の管理者を定めておく。

①ネットワークキー
②SSID（又は ESSID）
③認証情報
④AP の設定時に使用する ID、パスワード

(4)無線 LAN 子機の管理

無線 LAN 子機は、盗難防止等を考慮して、パソコンやデバイス内蔵のものを使用することが望ましい。無線カードや無線 USB 子機をパソコン等に接続して無線 LAN を利用する場合は、盗難・紛失しないように子機の管理を行う。

(5)電波干渉、カバレッジホールの回避

AP は通信できる範囲に制限があるため、それを超えるエリアの無線 LAN を構築する場合は、複数の AP を設置する必要がある。そのため、周囲のオフィス等で AP がすでに設置されているケースや、事務所内に複数台の AP を設置する場合は、電波干渉や電波の届かないカバレッジホールが発生しないように設置場所に注意する。特に、2.4GHz 帯ではこの現象が発生しやすいので、5GHz 帯を活用することで解決する可能性が高い。

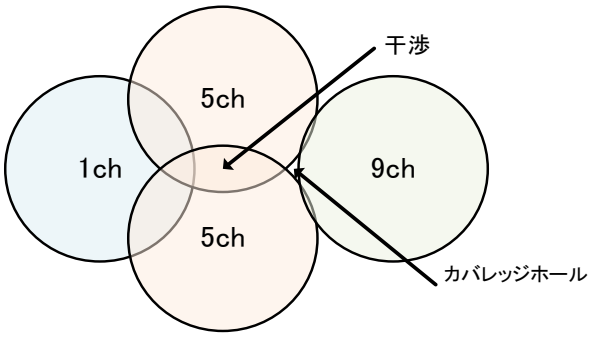

図 4-3　無線 LAN における電波干渉エリアとカバレッジホール

(6)AP への電気供給

電波は、障害物の少ないところの方がより遠くまで届きやすいため、AP を高い位置へ設置するケースが多くなる。しかし、一般的にコンセントは壁の低い位置に設置されているため、AP の電源確保が難しくなる。その場合は、PoE 対応ネットワーク機器を用いることにより LAN ケーブル経由で電気を供給できる。

4.4　共有サーバー（NAS）利用時の対策

現場内に共有サーバーを設置する場合、サーバー管理者を決め、以下のようなセキュリティ対策に留意し運用を行う必要がある。

(1)ユーザーの管理

ユーザーの管理については、利用実態に合わせた適切な設定を行う。

①異動等により不要なユーザーIDが生じた場合、速やかに削除する。

②管理者権限を有するアカウントやユーザーIDのパスワードについては、類推し難いパスワードを設定し、定期的な変更を行う。

③可能な限り、共用IDの作成を行わないようにする。やむをえず、共用IDが必要な場合、そのIDの利用者及び利用期間を台帳等に記録する。

④異動等で共用IDの利用者変更があった場合は、その共用IDのパスワードを変更するなどセキュリティ対策を行う。

(2)フォルダーのアクセス権

共有サーバーへのアクセスは、必要最低限の利用者やグループに限定する。

①フォルダーの用途や利用グループに応じ、適切なアクセス権を設定する。例えば、現場内限定、JV構成各社内限定、設計事務所限定、協力業者限定など。

②管理者は、アクセス権の付与状況を把握し、職員の異動やグループに変更が生じた場合、速やかに変更を行い周知する。

(3)ウイルス対策

共用データのウイルス感染防止、建設現場ネットワーク全体へのウイルス感染防止のため、共有サーバーにはウイルス対策ソフトを導入し、適切な運用を行う。

① ウイルス対策ソフトを導入し、常時稼働させる。
ウイルス対策ソフトは、パソコンで利用している製品とは異なる製品を採用することが望ましい。

② ウイルス対策ソフトやパターンファイルは、常に最新の状態に更新する。

③ OSのセキュリティ修正プログラムについては、その更新状況をチェックし、適宜適用する。

④ ウイルス対策ソフトが導入できない共有サーバーは、ウイルス対策ソフトが導入されているパソコンからネットワークドライブとして割り当て、ウイルス対策ソフトの検索対象にする。

(4)サーバーデータの保護

サーバーの誤操作・故障やウイルス感染からデータを保護するため、データのバックアップやサーバーの障害対策を行う。

①データのバックアップについては、バックアップすべきデータやバックアップ方法を検討の上、現場の状況に合わせた方法で行う。

②バックアップデータをメディアで保管する場合、鍵のかかるロッカー等へ保管するなど保管場所に注意する。

③障害対策としてUPS（無停電電源装置）の導入やミラーリングなどのRAID（Redundant Arrays of Inexpensive Disks）を必要に応じて構成し、耐障害性の向上を図る。

(5)盗難防止対策

重要な情報を管理する共有サーバーには適切な盗難防止対策を行う。

①共有サーバーは、入室者が限定され常時施錠された部屋へ設置することが望ましい。

②鍵付きのワイヤ等で事務机等に固定する。

③盗難や紛失等が発生した場合に備え、パスワード付きファイルの利用や暗号化等の対策についても必要に応じて実施する。

4.5　スマートデバイス利用時の対策

スマートデバイスは、利便性は高く誰もが使う、なくてはならないツールになっている。しかし、セキュリティに関しては個人的な利用を前提としていたことから、企業が業務利用する場合に要求するレベルのセキュリティ機能は備えていない。具体的には、個人利用の場合、主な使い道は、個人の生産性向上のための『メール・メッセンジャー／スケジュール／アドレス帳』であり、ほぼ100%の利用者がフリーのクラウドサービスを利用し、データ連携を行っているのが実情である。一方、企業での利用については、スマートデバイスの性格上、携帯電話としての管理と同時にモバイル PC としての両面からの管理を行う必要がある。

(1)携帯電話としての管理（携帯電話回線を利用している場合）

①紛失・盗難対策として、必ず首などに掛けられるストラップ付のケースなどを利用する。

②キーボードロック等のパスワードの設定・変更を義務づける。

(2)企業間でセキュリティポリシーが異なる場合の対応。

作業所におけるスマートデバイスの利用については、各社で定めたセキュリティポリシーの遵守が最低ラインとなる。利用にあたっては作業所の無線 LAN アクセスポイントの構築を含め、各社の情報セキュリティ担当部門に依頼し許可を得る。また、構成会社間でポリシーが異なる場合は、協議する。（よりセキュリティレベルの高い側に合わせる。あるいは、スポンサー会社のポリシーに従う。）

(3)スマートデバイスに関するセキュリティ対策の具体例

①レベル 1：最低限のルール策定とルール遵守の誓約

・脱獄（Jailbreak）しない、パスワード設定とローカルワイプ、ウイルス対策
・現場に関する情報のクラウドを介したデータ連携の許可／不許可
・現場内ネットワークへの接続の許可／不許可
・カメラ・音声レコーダー・GPS の使用許可／不許可と、許可された場合のデータ取扱いルール
・クラウドとの連携、意図しない同期の防止
（グーグルマップ／グーグルフォト等）

②レベル 2：最低限のルールの強制

・MDM（モバイル端末管理）により機能の制限に強制力を持たせる

③レベル 3：セキュリティ要件を満たすアプリケーションの利用

・スマートデバイス上には一切情報を保存しない
・保存データは暗号化され、かつ特定のアプリケーション環境内に閉じている
・DRM（利用権管理機能）によりデータ自体の期限設定やリモート削除を行う

4.6　バックアップ・リカバリー対策

故障やウイルス感染等により、パソコンやサーバーが使えなくなることがある。また、盗難や自然災害等により、機器そのものが消失してしまうことも考えられる。そういった不慮の事故に対応するために、データのバックアップが重要である。

(1)現場事務所内でのバックアップ

①共有サーバーのバックアップ

・NAS の場合
RAID はハードディスクの耐障害性を向上させるだけであり、機器自体の故障には対応できないのでバックアップは必要である。NAS に接続された外付けハードディスクやバックアップ用の NAS に、スケジューリング機能を使って自動バックアップする。

・パソコンの場合
容量が大きい外付けハードディスクに定期的にバックアップする。

②個人パソコンのバックアップ

ローカルディスクに保存されているデータは、定期的に各自がUSBメモリや外付けハードディスク等にバックアップする。

①②ともに、バックアップ媒体は、盗難や紛失に備えてデータの暗号化機能を搭載した製品が望ましい。

(2)現場事務所外へのバックアップ

機器の盗難・災害対策として、本支店に設置されているサーバーへのバックアップやクラウドの利用が考えられる。クラウドの利用に関しては、「6.　外部との情報共有（クラウドサービスの利用)」を参照のこと。

4.7　Webカメラ利用時の対策

Web カメラにはパソコンと直接接続して使用するものと、LAN やインターネットからの参照が可能なものがある。本ガイドラインでは、現場の監視や施工状況の映像共有といった目的のために、LAN やインターネットからWebカメラを利用する際の対策について述べる。

(1)インフラについて

①LAN内で使用する場合

設計事務所や協力業者等とLANを共有している場合は、目的に応じてカメラによる映像共有範囲を定め、適切なセグメントに配置する。また、Webカメラを無線LANで通信する場合は、盗聴に注意する必要がある。対策方法については、それぞれ「4.1 LAN共有時の対策」「4.3　無線LAN利用時の対策」を参照のこと。

②インターネット経由で使用する場合

インターネット経由で直接Webカメラを利用する場合、現場事務所LANとは別のインターネット回線を別途用意する。この場合、プロバイダーと固定グローバル IP アドレスサービスを契約するか、独自 URL を取得し、DynamicDNS サービスを利用するなどの対応を行う。また、ルーターにはポートフォワーディングの設定を行う。いずれの場合も独自運用する場合は、セキュリティ対応が脆弱になる可能性が高いため、できるだけ、カメラメーカーのサービスやベンダーのソリューション等を利用することが望ましい。

③動画など大容量データを配信する場合

ネットワーク回線の負荷が懸念される場合、別途、独立したインターネット回線を敷設するなど、対策を検討／実施する。

(2)Webカメラについて

①Webカメラへ設定又は操作のためにWebブラウザからアクセスする場合、暗号化通信に対応した機器を用意する。

②無線LAN対応のWebカメラの場合、「4.3　無線LAN利用時の対策」に挙げたセキュリティ設定が可能な機器を用意する。

③Web カメラの設定画面へアクセスする場合、ID、パスワードでの認証を行い、管理者以外は設定できない様にしておく。

④Webカメラ、ソフトウェアおよびファームウェアは、最新版を適用する。

⑤インターネットから首振り、ズーム等の遠隔操作ができる場合、近隣と接する現場ではプライバシーに配慮し、周辺住居など施工現場とは関係ない場所が映らないよう、カメラを設置するか、首振り範囲の設定が可能なカメラを使用する。また、必要に応じて遠隔操作機能を停止し、スナップショットによる公開など設定変更を行う。

⑥公開目的によっては、閲覧制限を設ける。

⑦防犯、発注者・設計者による監視又は災害監視目的を除き、録画は原則行わない。録画を残す場合はデータを厳重に保管し、個人情報保護法に抵触しないよう留意する。

(3)Webカメラの接続例

Web カメラの接続例を図 4-4 に示す。

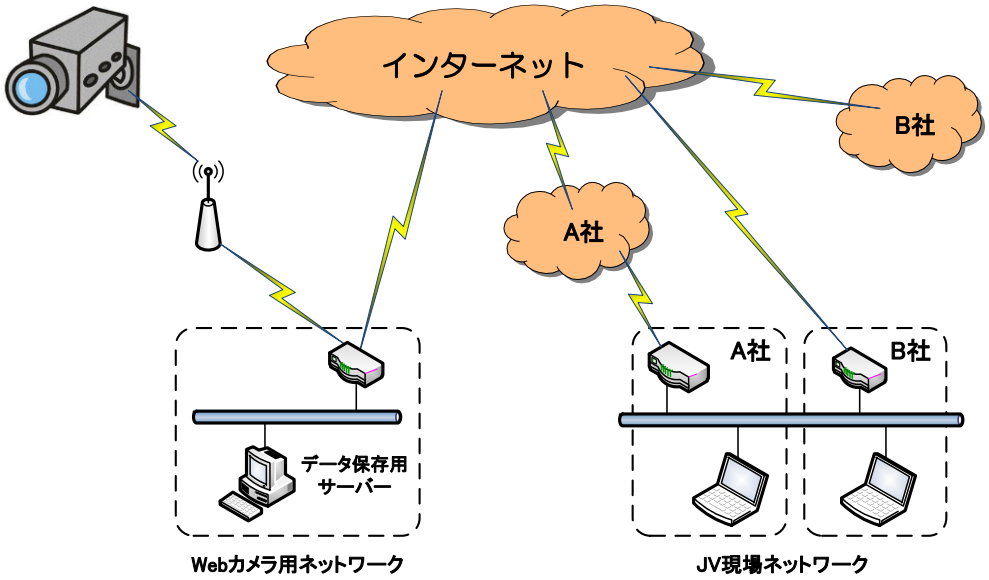

図 4-4　Web カメラ接続例

5. ＪＶ現場ネットワーク構築手順と事例

本ガイドラインを活用し、JV 現場ネットワークを構築する標準的な手順及び事例を以下に示す。この手順、事例は参考例であり、実際の各 JV の要件等によって、合理的な変更等を規制するものではない。

5.1 手順

手順 1 最初の JV 運営委員会開催時での運営方法の提示

幹事会社は、最初の JV 運営委員会において「JV の運営方法」を協議する際に、「JV 現場内の情報共有運営方法」を議題として掲げ、本ガイドラインに沿った下記項目を提示する。

事前に各構成会社からある程度の情報を収集しておくことが望ましい。

①おおよそのシステム構成（1 セグメントについて、サーバー設置について）

②ネットワーク担当者の選定（付録-1 の様式-2 参照）

③機器、ソフト類を各社で準備するか JV で準備するか。その場合の機種やソフトウェアのバージョン等。

④費用負担（付録-1 の様式-3 参照）

⑤覚書の内容（付録-2 参照）

必要に応じて、本件の詳細事項については、次回以降、JV 運営委員会に代わる実務レベルでの会での決定に委譲する等の決定をしておくことが望ましい。

手順 2 構成各社における検討

構成各社は、幹事会社が提示した運用方法（①～⑤）による運営が可能か各社の情報セキュリティ管理部門に照会し、「合意できない」場合は、「どの部分に問題があり、どのように変更すれば良いか」を確認する。第２回 JV 運営委員会若しくはそれに代わる会の開催前に幹事会社に、問題点と変更希望内容を通知する。

幹事会社から運用方法（①～⑤）が提示されない場合は、構成会社から提示する。

手順 3 JV 内調整（第 2 回 JV 運営委員会若しくはそれに代わる会の開催時）

第２回 JV 運営委員会若しくはそれに代わる会において構成各社の意向を調整する。

構成各社が、幹事会社が提示した運用方法（①～⑤）に則して運営できる場合は、幹事会社が主導的に「2.　ネットワーク構成」以降の事項を確定する。

構成各社の中で合意できない会社がある場合は、合意できない箇所のみ協議し、調整を図った上で、幹事会社が主導的に「2.　ネットワーク構成」以降の事項を確定する。

手順 4 管理資料の策定

全ての項目が確定した段階で、幹事会社は、運用方法（①～④）について管理資料を策定し、維持する。（付録-1 の様式-1～3 参照）

手順 5 覚書の締結

覚書を締結する。（付録-2 参照）

手順 6 運用（機器増設・撤去、各種管理業務）

各種機器増設、ネットワーク拡張等に伴い、管理資料メンテナンス及び必要に応じた協議・報告等を、幹事会社のネットワーク担当者、各構成会社のネットワーク担当者間で実施する。

JV 現場閉鎖の場合、廃棄パソコン等がある場合はそのデータの完全消去、記憶媒体等の処分、回線等の解約、各種資産（ルーター等）の引き取りを適切に行う。

5.2 事例

前節の手順を以下の事例にて JV 現場ネットワーク（LAN）構成図（1）～（3）及び各種管理資料の具体例を示す。なお、以下の表及び各種管理資料は、JV 現場ネットワーク（LAN）構成図（1）に基づくものである。JV 現場ネットワーク（LAN）構成図や各種管理資料に記述されている名称、金額等の値については全て架空であり、実在の商品や特定の価格等を示すものではない。

表 5-1　JV 構成例

SP、SB 区分	会社名	構成要素	備考/割当 IP アドレス
SP	幹事会社Ａ	ブロードバンド回線 PC5 台（PC 名、幹事会社Ａ1～5）	幹事会社 192.168.1.20～29
SB	構成会社Ｂ	ブロードバンド回線 PC2 台（PC 名、構成会社Ｂ1～2）	192.168.1.30～39
SB	構成会社Ｃ	ブロードバンド回線 PC3 台（PC 名、構成会社Ｃ1～3）	192.168.1.40～49
－	共通	ファイル共有サーバー1 台、ネットワークプリンター1 台	192.168.1.10～19

この事例では、インターネット接続にブロードバンドルーターを利用し、各構成会社に接続した例をあげているが、各構成会社間の事前協議において、アクセス回線等を安全に共用できると合意した場合は共用しても良い。

JV 現場ネットワーク構成図（1）～（3）を構成図例として以下に示す。特徴等は以下のとおり。

表 5-2　各構成図の特徴

構成図区分	説明
JV 現場ネットワーク（LAN）構成図（1） 【１セグメント型】	JV 内を１セグメント化している一般的な構成例
JV 現場ネットワーク（LAN）構成図（2） 【複数セグメント型】	ルーターを簡易 F/W として、各構成会社のセグメントを分割し、共有資源へのアクセスを確保しつつ「JV 現場ネットワーク（LAN）構成図（1）」より高いセキュリティレベルを保つ。
JV 現場ネットワーク（LAN）構成図（3） 【VLAN 対応ハブ導入型】	VLAN 対応ハブを導入してセグメントを分割し、共有資源へのアクセスを確保しつつ高度なセキュリティレベルを保つ。

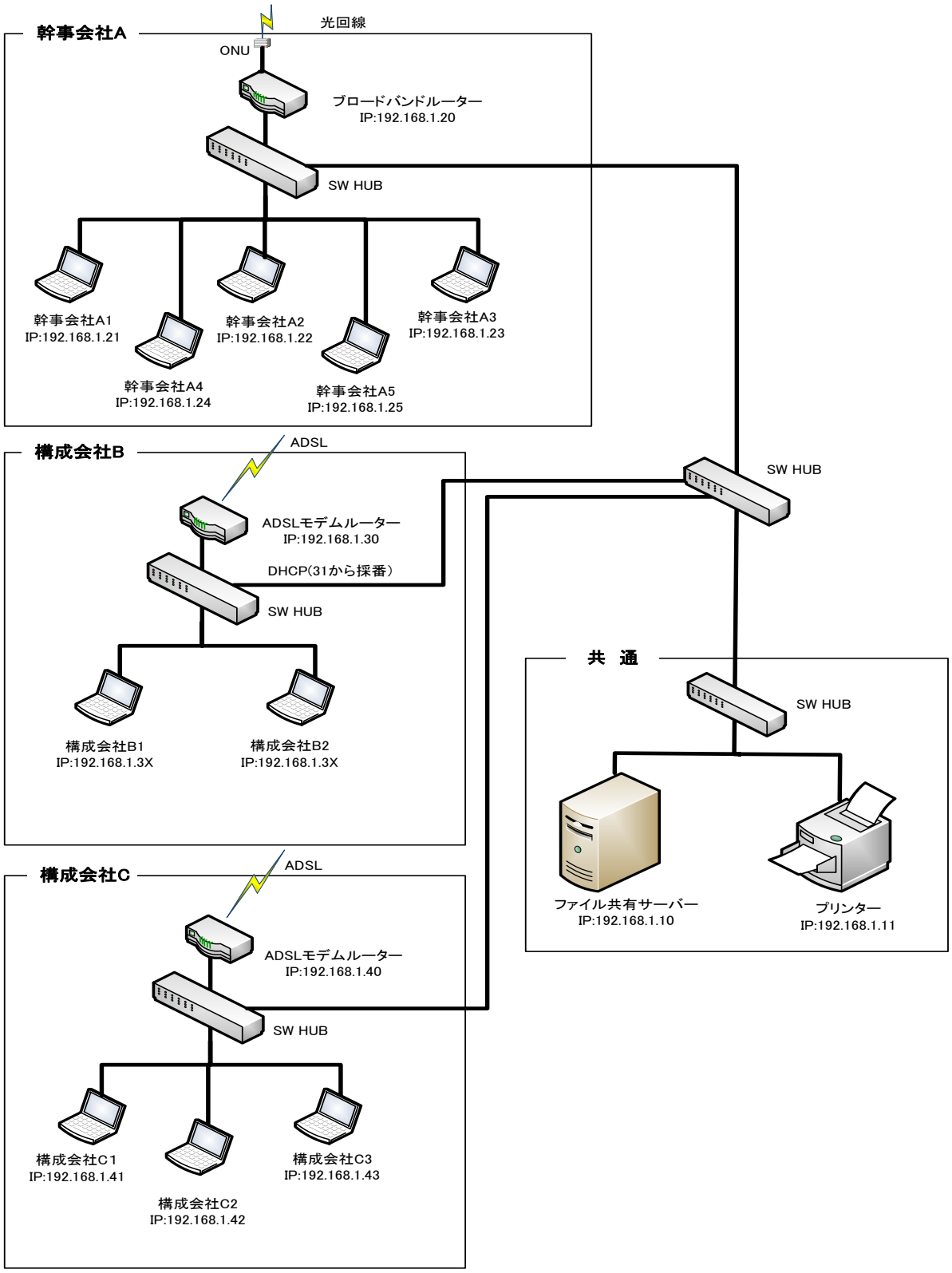

図 5-1　JV 現場ネットワーク（LAN）構成図(1) 1 セグメント型

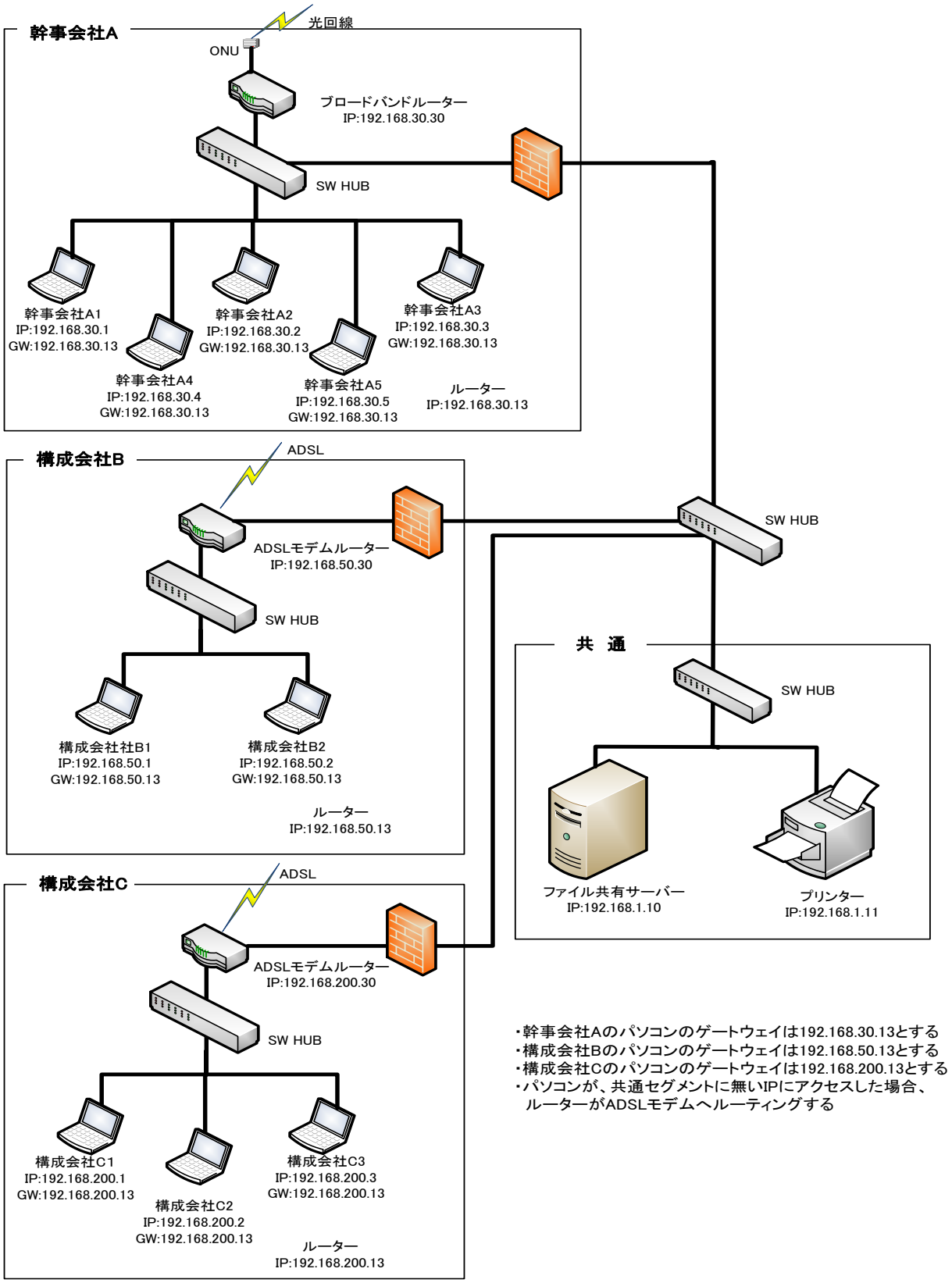

図 5-2 JV 現場ネットワーク(LAN)構成図(2) 複数セグメント型

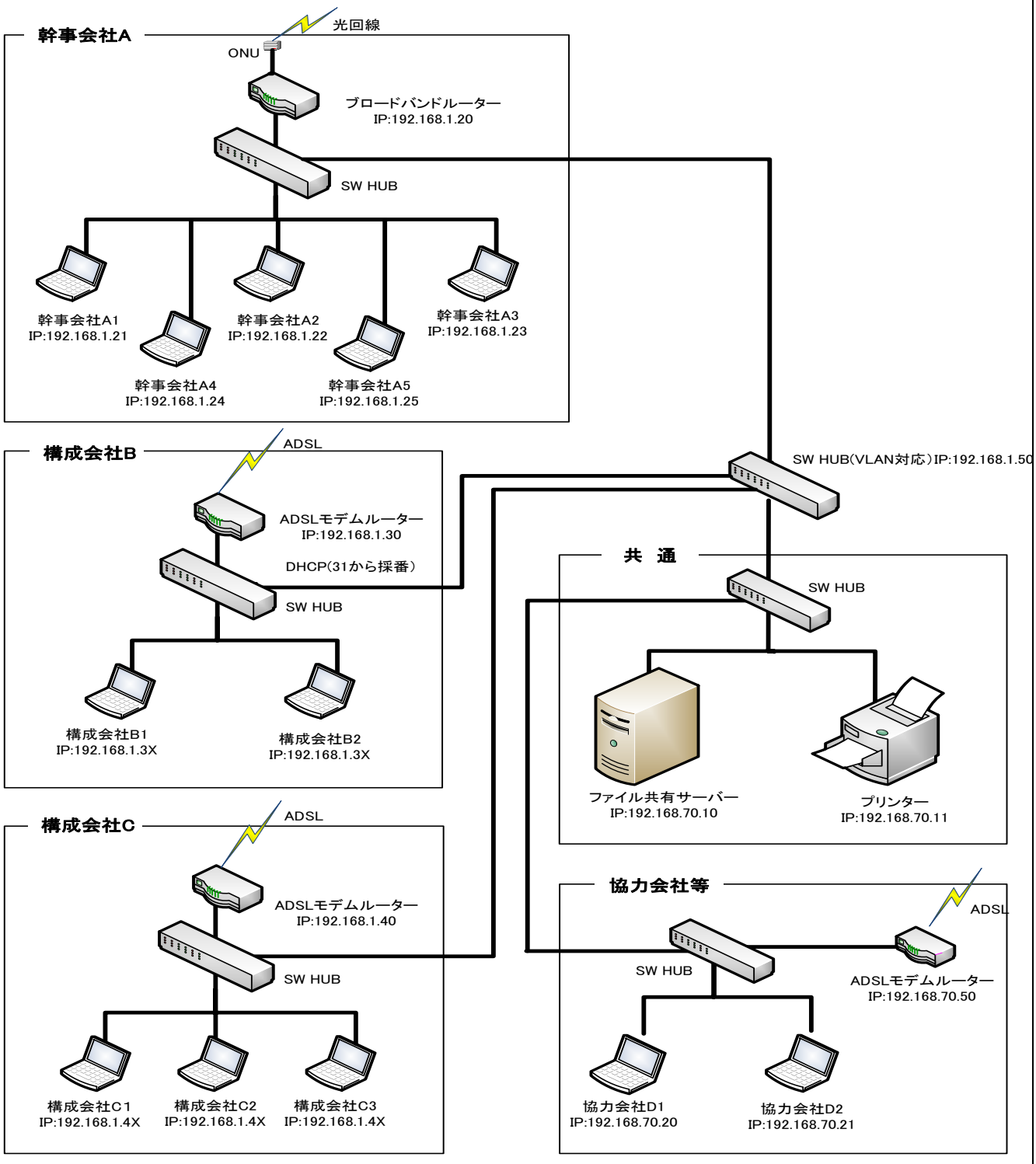

図 5-3 JV 現場ネットワーク(LAN)構成図(3) VLAN 対応ハブ導入型

ネットワークアドレス一覧表

IP アドレス	利用機器	コンピューター名	所属/利用者	採番	備考
192.168.1.10	ファイル共有サーバー	JV1	JV（幹事会社 A）	固定	共有名：shr
192.168.1.11	ネットワークプリンター	JV2	JV（幹事会社 A）	固定	共有名：prn01
192.168.1.20	ブロードバンドルーター	－	幹事会社 A	固定	
192.168.1.21	パソコン	幹事会社A1	幹事会社 A A社員 1	固定	
192.168.1.22	パソコン	幹事会社A2	幹事会社 A A社員 2	固定	
192.168.1.23	パソコン	幹事会社A3	幹事会社 A A 社員 3	固定	
192.168.1.24	パソコン	幹事会社A4	幹事会社 A A 社員 4	固定	
192.168.1.25	パソコン	幹事会社A5	幹事会社 A A 社員 5	固定	
192.168.1.30	ブロードバンドルーター	－	構成会社 B	固定	DHCP サーバー
192.168.1.3x	パソコン	構成会社 B1	構成会社 B B 社員 1	DHCP	31 から採番
192.168.1.3x	パソコン	構成会社 B2	構成会社 B B 社員 2	DHCP	
192.168.1.40	ブロードバンドルーター	－	構成会社 C	固定	
192.168.1.41	パソコン	構成会社 C1	構成会社 C C 社員 1	固定	
192.168.1.42	パソコン	構成会社 C2	構成会社 C C 社員 2	固定	
192.168.1.43	パソコン	構成会社 C3	構成会社 C C 社員 3	固定	

注）その他のネットワークパラメータ
・デフォルトゲートウェイ：各構成会社への接続ルーターの IP アドレス
・サブネットマスク：255.255.255.0
・DNS サーバー：各構成会社が指定する DNS サーバーの IP アドレス
（作業所内の名前解決は、ブロードキャストあるいは hosts、lmhosts ファイルによる）
〈項目説明〉
＊IP アドレス：C クラスのプライベートアドレスを利用する
＊利用機器：ルーター等のネットワーク機器、パソコン、ファイルサーバー、ネットワークプリンターなど
＊コンピューター名：ネットワーク上の識別名
＊所属/利用者：構成会社、JV、パソコンの場合は利用者を記入する
＊採番：固定／DHCP／－（関係なし）
＊備考：その他、ネットワーク条件を付記する

JVNW 様式-2

各社ネットワーク担当一覧表

構成会社	氏名	所属	電話番号	電子メール	備考
幹事会社 A	鈴木一郎	ABC-JV	03-xxxx-xxxx	isuzuki@a.co.jp	幹事会社
構成会社 B	佐藤二郎	本社総務部	03-yyyy-yyyy	jsato@b.co.jp	
構成会社 C	高橋三郎	支店管理部	03-zzzz-zzzz	takahashis@c.co.jp	

〈項目説明〉

＊構成会社、氏名、所属、電話番号、電子メール：各社ネットワーク担当を記入する

＊備考　　：幹事会社等を明記する

JVNW 様式-3

情報処理関連設備の費用分担表

項目		費用負担	費用（円）	備考
ハード	パソコン、ディスプレイ	共通原価	7,000	月額使用料
	ルーター	共通原価	70,000	買取
	サーバー	共通原価	30,000	月額使用料
	プリンター	共通原価	4,000	月額使用料
ソフト	JV内共通ソフト	共通原価	60,000	買取
	構成会社独自ソフト	構成会社	20,000	買取
通　信	LAN配線	共通原価	150,000	当初設置費
	通信回線	共通原価	30,000	月額使用料
	通信設定	共通原価	30,000	当初設置費
サポート	保守契約	共通原価	10,000	月額使用料

〈項目説明〉

＊費用負担　　：それぞれについて「共通原価／構成会社」を選択する

＊費用　　：それぞれの設備の月額又は一時費用

6.　外部関係者との情報共有（クラウドサービスの利用）

発注者、設計者や、協力会社等の外部関係者とネットワークを介して情報共有を行うケースが増えている。建設現場ネットワークの環境で外部関係者と情報共有を行う場合は、クラウドサービスの利用を前提とする。

クラウドサービスはサービス提供会社が利用目的に応じて各種サービスを提供しており、比較的容易にサービスの利用が可能である。

一方で、利用にあたってはクラウドサービスならではの利用上の留意点がある。本章では、外部関係者との情報共有手段としてのファイル共有サービスやメッセージングサービスの利用を想定したクラウドサービスの利用上の留意点を解説する。

6.1　利用イメージと利用可能サービス

クラウドサービスは、各利用者がインターネットを介してクラウドサービス事業者のサーバーにアクセスすることにより、情報の共有や各種サービスを利用する。

クラウドで利用可能な情報共有サービスは、ファイル共有やメッセージングサービス、テレビ会議システム等、数多くある。

利用にあたっては、利用者がインターネット接続環境を準備し、サービス提供会社が定めた利用規約に則って利用する。

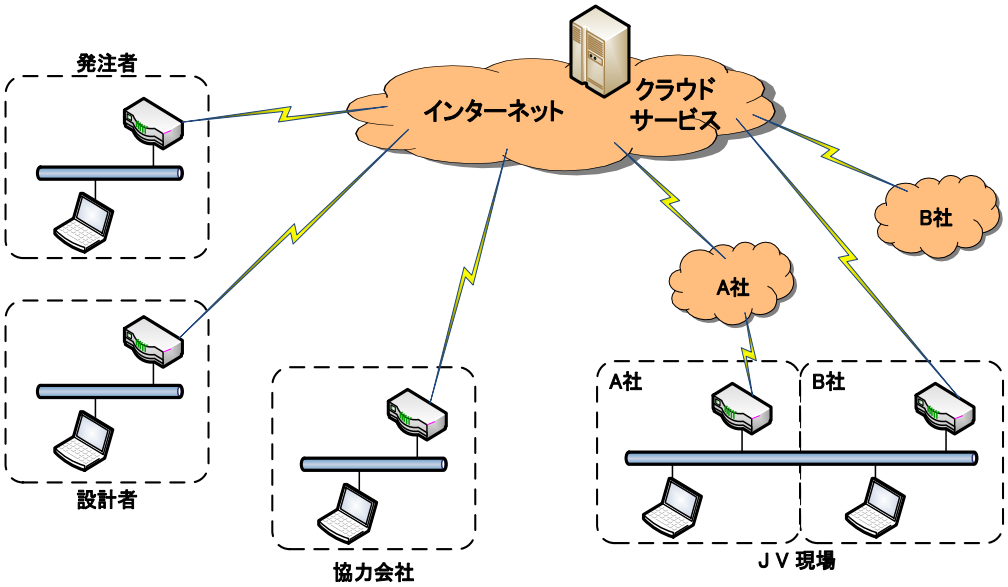

図 6-1　クラウドサービスの利用イメージ

6.2　利用にあたっての注意事項

クラウドサービスは、データがサービス事業者の用意するサーバー上に保管されることに加えて、インターネットを介してデータが交換されることから、十分なセキュリティ対策が施されたサービスを選択することが重要であり、かつ利用にあたっては発注者の許可を得ることが前提となる。

特に安価なサービスや無料のサービスは、サービスの信頼性やセキュリティ対策等が十分であるかの評価が必要で、安易に利用すべきではない。

クラウドサービスを利用する際には、サーバーが所在する国や地域にも留意する必要がある。クラウドサービスのサーバーが海外に設置されている場合には、その国や地域の法律や規則、捜査権等が及ぶ場合があるため、そのリスクも考慮する必要がある。

また、発注者等からの要請により、自社の基準よりもセキュリティレベルが低いサービスを利用しなければならない場合も考えられる。このような場合、万一の情報漏洩事故に対する責任の所在を事前に

明確にしておくこと必要がある。
クラウド上に保存したデータの帰属についても、保存データを利用できる権利をサービス事業者が有するケース等もあるため、利用規約のチェックを法務部門で受けることも考慮すること。
クラウドサービス上に保存したデータの管理責任は利用者側にあるため、情報が漏洩した場合は、原則、利用者の責任となる。なお、クラウド事業者が実施するセキュリティ対策は、クラウド事業者の責任範囲についての対策であるため「セキュリティ対策は万全」といった説明があったとしても、利用者側で情報漏洩を防止するセキュリティ対策の実施が必要となる。

6.3 サービス選定時の評価項目

(1)機能要件、コスト

クラウドサービスを選定するにあたっては、関係者と協議の上、以下の点に注意する。

・発注者・設計者等から禁止または指定のサービスがあるかを確認する。
・禁止または指定のサービスがない場合は、機能要件・セキュリティ要件・コスト等を考慮してサービスを選定する。

(2)提供者側のセキュリティ要件

提供者側のセキュリティ要件は、機密性（預けているデータやアカウント情報が外部に漏洩しない)、完全性（預けているデータが消失しない・アクセス記録が残る)、可用性（サービス停止しない）がある。以下にそれぞれの確認事項について挙げる。

・機密性（ユーザー認証方式、通信の暗号化、データの暗号化、アクセス権の設定等）
第三者機関によるセキュリティに関する認定を受けているか確認する。
アカウントの認証は成りすまし防止機能を備えているかを確認する
プロジェクトに参画している人間に必要な情報が開示され、プロジェクト外の人間には開示されていないことを管理できる機能を備えているか確認する。

・完全性（バックアップ、ウイルス対策、アクセスログ等）
データの保全性、アクセス記録の種類・保存期間について確認する。

・可用性（冗長化）
サービス停止の可能性、停止時のサービス利用料返還について確認する。

提供者側のセキュリティ要件については、「添付資料　クラウドサービスレベルのチェックリスト」も参考にしてもらいたい。

6.4 利用デバイスと情報漏洩対策

(1)利用デバイスの条件

クラウドサービスはパソコンやスマートフォンなど様々なデバイスからアクセスできることが当たり前になっているが、当該クラウドサービスを利用する上で、使ってよいデバイスの制限をかけるかどうかを検討する。
（パソコンはウイルス感染する前提で考える必要がある／スマートデバイスの場合は、Android は iOS よりリスクが高い）

(2)デバイスのローカル環境へのデータ保存の可否

パソコンやスマートデバイスのローカル環境にデータを保存してよいかどうかを検討する。
ローカル環境にデータを保存すると利便性はよいが情報漏洩のリスクが増す。一方で、ローカル環境にデータを保存させないと情報漏洩のリスクは下がるものの利便性は損なわれる。
情報漏洩のリスクを下げるためローカル環境に保存できないようにするか、セキュリティ対策をとった上でローカル環境に保存できるようにするか、決めておく必要がある。

(3)その他の情報漏洩対策

・個人アカウントの乗っ取りやパスワード流出対策
　２段階認証／パスワードの使い廻しをしない等の対策をとる。

・管理者 ID の保護
　管理者 ID は IP アドレス制限や端末制限をかけることが望ましい。どちらもできない場合は、多要素認証など認証を強化する。

6.5　運用管理体制の整備

クラウドサービスの利用にあたっては、運用管理体制を整備する必要がある。特に、プロジェクトで使用するクラウドサービスの運用に責任を持つ管理者の設置が必須である。

(1) 運用管理体制の目的

プロジェクトの関係者が必要なサービスを使うことができ、プロジェクト外の人間、特に以前プロジェクトに参画していたがその後プロジェクトから外れた元関係者等がサービスにアクセスできないよう管理する必要がある。

(2)管理者の役割

・利用上のルール（保存してよい情報の内容、使って良い機能など）を決め、利用者に周知、徹底する。提供されている機能の中で、情報漏洩リスクの高い機能※の利用は原則禁止する。利用する必要のない機能は誤操作の原因となるため、できる限り停止させる。

※情報漏洩リスクの高い機能：保存データを外部へ送信する機能（他のサービスとのデータ連携・データ共有、メールやメッセージ送信、エクスポート、ダウンロード機能など）

・保存するデータの所有者から利用許可を得る。
（デジタルデータには著作権、所有権が定義されないため、請負契約や秘密保持契約の内容からデータの所有者を判断して、クラウドサービスの利用について事前承認を得る。）
・アカウント管理／グループ管理／権限設定／ログ管理を行う。
・申請フロー　申請～承認～追加／変更／削除の手順を定める。
・アカウントやグループの登録状況は定期的に棚卸を実施する。
・定期的にログを確認し、不正なアクセスが発生していないことや、ルールに反した使い方がされていないか、設定が正しい状態であることを確認する。
・コスト管理を行い、定期的に価格とサービス内容とを見直す。

(3) 利用者の注意事項

・部署、現場で決めた利用上のルールを確認し、ルールに則り利用すること。
・パスワードを厳格に管理すること
　① パスワードは８文字以上とする。
　② パスワードは類推が困難なものとする。
　③ パスワードの使いまわしは禁止。
　④ 配布された初期パスワードは、そのまま利用せずに速やかに変更する。

6.6　利用するサービスに関する個別の注意事項

クラウドサービスにおいて、利用することが多いストレージサービスとメッセージングサービスについて個別の注意事項を記載する。

・ストレージサービスの固有の注意事項

a)プロジェクト終了時に、蓄積されたデータの扱いについて定めておく。

ストレージサービスはプロジェクト終了時には保存データが膨大になる。そのデータを削除するのか、移設するのか、ストレージサービス上にそのまま残すのか、を決めておく。

b) ウイルス対策

クラウドサービス上で社外の方とデータファイルを共有する場合は、クラウドサービス上でウイルス対策を実施する。クラウドサービス側にウイルス対策の機能が無い場合は、アップロード、ダウンロード時のパソコン側でウイルス対策を実施すること。

c)データ消失対策

利用者側の操作ミスや第三者の不正アクセスによるデータ消失の責任は、利用者側にある。データのバックアップは、利用者側で確実に実施すること。

・メッセージングサービスの固有の注意事項

a)利用するサービスの範囲を定めておく。

メッセージングサービスが提供するサービスは幅が広く、中には、画面共有やリモートコントロールまで行える機能を保有するものがある。必要な機能を見極めて、不要な機能が稼動していたために情報漏洩に繋がることのないようにしなければならない。

付　　録

付録-1　JV 現場ネットワーク管理資料ひな型
ネットワーク維持管理に用いる以下の管理資料のひな型を添付する。

様式-1　ネットワークアドレス一覧表
様式-2　各社ネットワーク担当者一覧表
様式-3　情報処理関連設備の費用分担表

付録-2　電子情報の取り扱い及びネットワークシステムに関する覚書（例）

付録-3　ＪＶ現場における無線 LAN 利用申請書（例）

付録-4
参考資料-1　用語解説（本書での用語定義）
参考資料-2　よくあるトラブルの要因
参考資料-3　電波法・電気通信事業法の説明

ネットワークアドレス一覧表

IP アドレス	利用機器	コンピューター名	所属/利用者	採番	備考
192.168.　　.					
192.168.　　.					
192.168.　　.					
192.168.　　.					
192.168.　　.					
192.168.　　.					
192.168.　　.					
192.168.　　.					
192.168.　　.					
192.168.　　.					
192.168.　　.					
192.168.　　.					
192.168.　　.					
192.168.　　.					

注）その他のネットワークパラメータ

・デフォルトゲートウェイ：各構成会社への接続ルーターの IP アドレス

・サブネットマスク：255.255.255.0

・DNS サーバー：各構成会社が指定する DNS サーバーの IP アドレス

（作業所内の名前解決は、ブロードキャストあるいは hosts、lmhosts ファイルによる）

〈項目説明〉

＊IP アドレス　　：C クラスのプライベートアドレスを利用する
＊利用機器　　：ルーター等のネットワーク機器、パソコン、ファイルサーバー、
　　ネットワークプリンターなど
＊コンピューター名：ネットワーク上の識別名
＊所属/利用者　　：構成会社、JV、パソコンの場合は利用者を記入する
＊採番　　：固定／DHCP／－（関係なし）
＊備考　　：その他、ネットワーク条件を付記する

付録-1

JVNW 様式-2

各社ネットワーク担当者一覧表

構成会社	氏名	所属	電話番号	連絡先（電子メール）	備考

〈項目説明〉

＊構成会社、氏名、所属、電話番号、連絡先（電子メール）：各社ネットワーク担当者を記入する

＊備考：作業所内担当者や構成会社の情報システム部等を明記する

情報処理関連設備の費用分担表

項目		費用負担	費用（円）	備考
ハード	パソコン、モニター	共通原価／構成会社		
	ルーター	共通原価／構成会社		
	サーバー（NAS）	共通原価／構成会社		
	プリンター	共通原価／構成会社		
	プロッター	共通原価／構成会社		
ソフト	JV現場共通ソフト	共通原価／構成会社		
	構成会社独自ソフト	共通原価／構成会社		
通　信	LAN配線	共通原価／構成会社		
	通信回線料金	共通原価／構成会社		
	通信設定工事	共通原価／構成会社		
サービス	機器保守	共通原価／構成会社		
	プロバイダー契約料	共通原価／構成会社		
	ASP料金	共通原価／構成会社		
	電子商取引サービス料	共通原価／構成会社		

〈項目説明〉

＊費用負担　　：それぞれについて「共通原価／構成会社」を選択する

＊費用　　：それぞれの設備の月額又は一時費用

電子情報の取り扱い及びネットワークシステムに関する覚書（例）

株式会社幹事会社Ａ（以下「甲」という。）、株式会社構成会社Ｂ（以下「乙」という。）、構成会社Ｃ株式会社（以下「丙」という。）（以下甲・乙・丙を総称して「構成員」という。）とは、○○○○年○○月○○日付にて構成員間で締結した共同企業体協定書に付帯して、共同企業体内での電子情報の取り扱い及びネットワークシステムに関し、以下の事項について合意した。

第１条　目的

本覚書締結は共同企業体内での電子情報の取扱い及びネットワークシステムに関わる不正行為を防ぐことを目的とする。

電子情報の取扱い及びネットワークシステムに関わる行為を以下に示す。

①共同企業体内での電子的な情報交換。

②構成員の自社の企業内ネットワークへの接続。

③発注者、設計者、コンサルタント、協力会社及び自社本支店等とネットワークを介しての電子的な情報交換。

第２条　責任と役割

1　構成員は、共同企業体内で情報共有を行なうに当たり、本覚書締結事項を遵守し、信義を重んじ誠実に運用にあたらなければならない。

2　構成員は、業務の遂行上知り得た共同企業体及び自社以外の業務上の秘密情報及び技術情報などを第三者に開示、漏洩又は提供してはならない。

3　構成員は、本条を遵守させるために必要な措置を講ずるものする。

4　本条の規定は、共同企業体解散後も効力を有するものとする。

第３条　禁止事項

構成員は、以下に定める事項の遵守を徹底しなければならない。

①共同企業体内の他の構成員固有データの盗用・破壊・改ざんの禁止。

②共同企業体内固有データの業務外使用の禁止。

③他の構成員が保有する独自システムへの侵入禁止。

④上記に定める事項のほか、別途運営委員会で制定した禁止事項。

第４条　違反時の処分規定

構成員が本覚書において定めた事項に違反した時は、当該構成員は運営委員会の決定した処分に従わなければならない。

第５条　その他の取決め

構成員は、本覚書並びにガイドラインに定めのない事項又は疑義のある事項が生じたときは運営委員会において定めるものとする。本覚書の全部又は一部を変更する場合も同様とする。

上記締結の証として、本覚書３通を作成し甲・乙・丙記名押印の上、各々１通を所有するものとする。

○○○○年○○月○○日

甲

＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿

乙

＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿

丙

＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿

JV現場における無線LAN利用申請書(例)

xxxx 年 xx 月 x 日

○○○○○○JV 工事事務所
所長殿

株式会社　○○○○○○

○○○○職員にタブレット端末を利用させる件（依頼）

当社では生産性向上、業務の効率化を目的に当社現場職員に対し、タブレット端末の利用を展開しております。タブレット端末の利用にあたってはネットワークへの接続が必須となりますが、同機は無線 LAN 接続にしか対応していません。

一般社団法人　日本建設業連合会(日建連)では「建設現場ネットワークの構築と運用ガイドライン」にて無線 LAN の利用にあたり、「一部でも無線 LAN を導入する場合には、JV 現場ネットワーク全体のセキュリティに影響を与えるため、導入前には JV 構成会社全体の承諾を得る。」と規定されており、今回本ガイドラインに則り、無線 LAN での接続を許可頂きたくお願いするものです。

なお、今回設置を希望する無線 LAN 機器は、配布するタブレット端末に「電子証明書」を搭載したものからのアクセスしか受け付けない仕様で、現段階で無線 LAN の接続では最も安全な方式となっております。

つきましては、下記の通り無線 LAN 環境を構築したくご検討願います。

記

1　設置する無線 LAN 機器
　○○○○製　○○○○

2　無線 LAN 接続時の認証方式
　WPA2 エンタープライズによる認証

※「WPA2 エンタープライズ」とは
通常、無線 LAN に接続する場合には SSID と呼ばれる ID とパスワードが漏洩した場合第三者が不正にアクセスできる可能性があります。WPA2 エンタープライズは当社内に設置されたサーバーが発行する「電子証明書」をタブレット端末にインストールし、この電子証明書で認証を行います。したがって ID、パスワードによる認証は行なっていません。また電子証明書はコピー又は偽造することができないため、現段階で無線 LAN の接続では最もセキュアな認証方式です。

3　タブレット端末のセキュリティ対策
万一の盗難、紛失に際しては、取得者がタブレット端末を利用できないようパスワードによるロックを必須とし、規定回数以上の入力ミスがあった場合は、タブレット端末上のデータを全て削除する対策を講じています。また、暗号化機能を有効にし、MDM(モバイルデバイスマネージメント)の採用により、ネットワーク接続下でリモートワイプ、リモートロック機能によりデータを保護・削除します。

4　本件に関する問い合わせ先及び資料提出先
　株式会社○○○○
　Tel :　　Mail :

以上

参考資料-１　用語解説（本書での用語定義）

1. ネットワーク機器

ネットワーク機器には、ハブ、ルーター等の通信機器がある。

(1)ハブ（スイッチングハブ）

ネットワークの中継機器であるハブの一種。送られてきたデータを解析し必要なポートにしかデータを送信しない。このため、ネットワーク全体の負荷が軽減し、セキュリティが向上する。

規格名	通称	最大通信速度	LAN ケーブル
1000BASE-T	ギガビットイーサ	1G(1000M)bps	カテゴリ 5e 以上
100BASE-T	ファストイーサ	100Mbps	カテゴリ 5 以上
10BASE-T	ー	10Mbps	カテゴリ 3 以上

【注意点】

ギガビットイーサは、サポートしている製品とサポートしていない製品があるので、確認が必要。

スイッチングハブでは、転送先を最適化するため、IP アドレスと MAC アドレスを自動学習する。そのため、端末の接続位置を変更したり、ネットワークカードを交換したりした場合に、通信できなくなることがある。このような場合には、端末の再起動だけではなく、スイッチングハブの再起動も必要となる。

(2)ルーター

ルーターとは、複数の異なるネットワーク間でデータのやりとりを中継するための機器。ルーターはネットワークアドレスを元に、管理者が意図する経路でデータ（パケット）を配送したり、ルーター自身が経路を自律的に選択して適切な配送を行なったりすることができる。また、フィルタリング機能により特定のアドレスのパケットを破棄してしまうことで、不正アクセスを制限するファイアーウォールとしても機能する。

【注意点】

ネットワークへの外部からの不正接続を防ぐため、一般的に危険な(弱点となる)ものだけでなく、必要でないポートは全て閉じる。

【注意点】

上記の各機器の特性を元に一般的には、ルーターを頭にして、その下位にハブを接続する。機器にはそれぞれの役割があり、これを無視して適当に接続してしまうとトラブルの原因となる。

2. VLAN：http://www.infraexpert.com/study/vlanz1.html

VLAN（ Virtual LAN ）とは、物理的な接続形態とは独立して仮想的な LAN セグメントを作る技術。VLAN はスイッチ内部で論理的に LAN セグメントを分割するために使用される。

3. クラウドサービス

インターネットを介して提供されるサービスのこと。基本的には、サービス提供会社がサーバーやアプリケーション、データ領域までの一式全てをサービスとして提供する。

4. NAS（Network Attached Storage; ネットワーク接続ストレージ）

NAS はネットワークに直接接続して利用する外部記憶装置（ストレージ）である。共有サーバーとほぼ同様であるが、ストレージとして専用化されているため設定や管理も容易である。高級機種では、RAID 機能やホットスワップ機能を有するものもある。

5. ファイアーウォール

組織内のコンピューターネットワークへ外部からの不正なアクセスや侵入を防止することを目的としたセキュリティシステムの総称。単純に IP アドレスや通信ポートによって許可／不許可を判断して通信制御する機器から、パケット内の情報よりアプリケーション情報まで判別して細かく制御する事が可能な機器まで幅広い種類がある。

参考資料−２　よくあるトラブルの要因

(1)ネットワークケーブル

ネットワークケーブルがうまく接続されていない場合が考えられるので、一度抜いてからカチッと音がするまで接続し直す。また、ネットワークケーブルは曲げに弱く、重いものがのったり、強く引っ張ったりすると断線する可能性がある。ハブのランプが点灯しているか確認して、点灯していない場合は、新しいケーブルに交換してみる。

(2)ネットワーク機器

ハブ等のネットワーク機器の電源ケーブルが抜けていないか確認する。また、ポートがひとつ故障した可能性もあるので、別のポートに差してみて確認する。次に、機器の故障した可能性もあるので、機器を交換して確認する。

(3)ハブのカスケード

ハブとハブをネットワークケーブルでつなぐことをカスケードという。カスケードによりポート数を増やすことができるが、古いハブでは接続台数には制限があるので注意すること。10BASE-T は 3 個、100BASE-T は 2 個。

スイッチングハブでは、カスケード接続台数に制限はない。

(4)コンピューター名

Windows ネットワークでは、コンピューター名でパソコンを識別するので、ひとつの LAN 上にコンピューター名を重複して設定出来ない。

(5)IP アドレス

同じ IP アドレスを 2 台のパソコンに設定してしまうと、ネットワーク全体に影響が出て、他のコンピューターが接続できなくなる。また、グローバルアドレスを間違って振ってしまうと、LAN の中の情報がインターネットに公開される危険性がある。

参考資料-3　無線 LAN 利用上の注意

電波法

- 2.4G/5G帯の無線LANの無線局は、電波法上の技術基準等を満たしており、かつ、技適マークがついている機器を使用する場合は、免許不要。

通称	周波数	免許の要否	主な運用形態
2.4GHz帯 無線LAN	2.4～2.497GHz	免許不要	主に屋内相互間 屋外移動 （～100m）
5GHz帯 無線LAN	5.15～5.35GHz 5.47～5.725GHz	免許不要	主に屋内相互間 屋外移動 （～100m） 5.15～5.35GHzは屋内限定

技適マーク

電波法（昭和25年法律第131号）
（無線局の開設）
第四条　無線局を開設しようとする者は、総務大臣の免許を受けなければならない。ただし、次の各号に掲げる無線局については、この限りでない。
一・二　（略）
三　空中線電力が一ワット以下である無線局のうち総務省令で定めるものであつて、次条の規定により指定された呼出符号又は呼出名称を自動的に送信し、又は受信する機能その他総務省令で定める機能を有することにより他の無線局にその運用を阻害するような混信その他の妨害を与えないように運用することができるもので、かつ、適合表示無線設備のみを使用するもの
四　（略）

電気通信事業法

- 公衆無線LANのアクセスポイントを用いて、利用者にインターネットに接続するサービスを事業として提供する場合は、原則として電気通信事業法上の届出（又は登録）が必要。

電気通信事業法（昭和59年法律第86号）
（電気通信事業の届出）
第十六条　電気通信事業を営もうとする者（第九条の登録を受けるべき者を除く。）は、総務省令で定めるところにより、次の事項を記載した書類を添えて、その旨を総務大臣に届け出なければならない。
一～三　（略）
2・3　（略）

＜出典＞総務省の HP より抜粋　http://www.soumu.go.jp/main_content/000152595.pdf

あとがき

ここ数年の情報通信環境の発展は目覚しいものがあり、今やほとんどの工事現場でコンピューターが利用されており、その大部分がインターネットに接続している状況である。

また、工事現場内の情報ネットワークも各社のネットワークとの接続は勿論のこと、受発注者間、協力業者間、更には、他業種間での情報共有へとの広がりを見せている。さらにはクラウドサービスやスマートデバイス等の新たな情報通信サービスの現場利用も増大しつつある。

このような傾向は今後ますます加速していくものと思われ、今後とも先進的な IT の調査を継続しつつ、時期に即した現場のネットワーク構築に有用な技術を本ガイドラインに反映すべく適宜改定を行っていく予定である。

2020 年 11 月の改定について

以下の改定方針に基づき、改定を行いました

１．時代に合わなくなった技術や機器について、今日のレベルに合わせた変更

２．建設現場の実運用状況を踏まえた運用ガイドラインの変更

３．サイバーセキュリティリスクに対応した対策案の変更

2024 年 2 月の修正について

「サプライチェーン全体のサイバーセキュリティ向上のための取引先とのパートナーシップ構築に向けて（令和 4 年 10 月 28 日経済産業省、公正取引委員会)」の遵守事項を追記

執筆委員：最新版（敬称略、五十音順）

奥田　由起憲(大林組)	小倉　弘至(清水建設)	川名　洋介(鹿島建設)
葛原　徹(大成建設)	高馬　洋一(安藤･間)	仙波　幹徳(三井住友建設)
滝沢　強(前田建設工業)	嶽野　聡(東急建設)	豆腐谷　洋一(竹中工務店)
長沼　秀明(戸田建設)	山口　正志(フジタ)	

執筆委員：初版

上村　昌弘（鉄建建設）	小澤　敦　（飛島建設）	葛原　徹　（大成建設）
日下　重次（鹿島建設）	高馬　洋一（安藤・間）	仙波　幹徳（三井住友建設）
丹治　弘典（清水建設）	津久井 啓介（大林組）	豆腐谷 洋一（竹中工務店）
鳥飼　裕之（奥村組）	長谷　芳春（三井住友建設）	長沼　秀明（戸田建設）
西牧　晋志（西松建設）	平井　明　（大成建設）	平原　昇　（東亜建設工業）
藤野　芳徳（前田建設工業）	山口　正志（フジタ）	

本書に関する問い合わせ先：

一般社団法人　日本建設業連合会　建築部

〒104-0032 東京都中央区八丁堀 2-5-1　東京建設会館 8 階

T　EL:03-3551-1118　FAX:03-3555-2463