建設現場ネットワークガイドライン

2001 年 04 月　初版
2024 年 12 月　改訂

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」との棲み分けを図って全面的に再編集した「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オンラインストレージ等の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。 なお、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、サーバーを利用した情報共有方法、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。 なお、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」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

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。

※留意事項

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）を遵守し、特に「第 3 取引先との関係構築」を留意すること。

URL: https://www.jftc.go.jp/dk/guideline/unyoukijun/cyber_security.html

２．建設現場のネットワーク構成

２．１　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

２．２　基本構成

建設現場ネットワークの全体にかかわるものを解説し、建設現場ネットワークを構成する主要 3 項目について、それぞれに解説をしていく。

(1) 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) 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。

(3) 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、スマートデバイス等のモバイル機器・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。

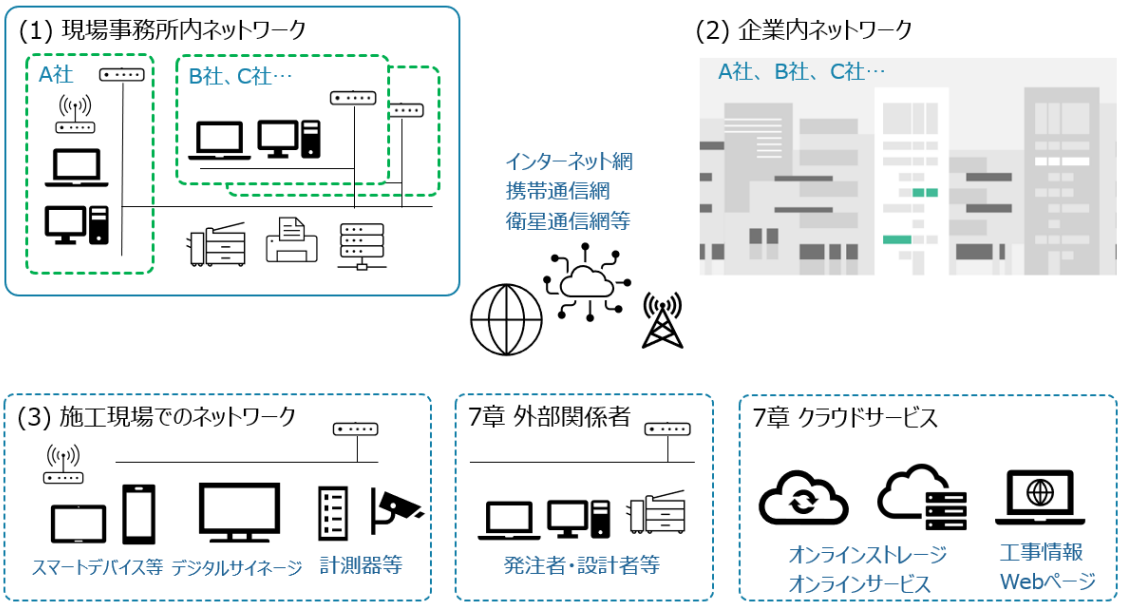

図１：建設現場ネットワーク　例

３．ネットワーク構成と要素

３． １　ネットワーク回線と基本構成

(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、「５． 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。

(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、JV 構成各社全てが SD-WAN（Software Defined-Wide Area Network）の利用や PC への EDR（Endpoint Detection and Response）の導入が完了している場合など、セキュリティ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。

(4) 企業内ネットワークへの接続

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。

(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。

(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、モバイル通信サービスが利用できる。

(7) 衛星通信サービスの利用

山間部や海上等で光回線やセルラー通信が利用できない工事では、衛星通信サービスが利用できる。

(8) 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。

(9) 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、「(8) JV 構成会社への接続」に準ずる。

(10) 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。

(11) 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、クラウドサービス（クラウドストレージ等）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、「７．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。

３．２　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、L2,L3 スイッチを利用した仮想 LAN やルーティングを利用するなど別途構成を検討する。

②JV 構成会社の IP アドレス体系の整合

VPN サービスを利用して各構成会社が各企業内ネットワークに接続する場合には、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

ネットワークを VLAN 構成とする場合、各 JV 構成会社に「16」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、「６．　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

DHCP の利用は建設現場ネットワークの構成によるため構成会社で協議する。 JV 構成会社全社が SG-WAN 利用を前提とする場合は 1 セグメント構成となるが、それ以外の場合については、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ったが、セキュリティ対応を実装したクラウドストレージサービスの利用も増えている。 共有サーバーの利用においては、多くのリスクがあり（盗難 破損・焼失 ファイル消失 バックアップ 監査ログ）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、マルウェア感染など、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（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、鍵のかかるサーバーラック等に収納する。

・クラウドストレージサービスを使う場合

クラウドストレージサービスは、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、「７．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、「５．４ 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、外部から共有サーバーにアクセスできるようにすることは基本的には禁止とする。ただし、共有サーバーOS 等のセキュリティアップデートのため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接続は可能としている。その場合は、社内の IT 専門部署や IT ベンダーに確認する必要がある。

(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 7 割程度にし、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。

３． 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 は各企業内で定められた IP-VPN 等を用いる。

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、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マルウェア感染

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

(3) モバイル通信サービスでの企業内ネットワーク接続

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機能を利用する。

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 で接続する。 少人数で共有可能である。

(4) JV 現場における回線の共有

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はアクセス回線を共有することができる。

通信事業者のサービスによっては、1 本の物理回線（光回線等）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、「５． ２ 回線共有利用時の対策」を参照のこと。

３． ４ 施工現場のネットワーク

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、施工現場においてもスマートデバイスが多く利用されている。 ここでは、施工現場ネットワークと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・スマートデバイス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、「５． ３ 無線 LAN 利用時の対策」「５． ５ スマートデバイス利用時の対策」を参照のこと。

①LAN ケーブルによる接続

施工現場と現場事務所が近接している場合は、有線 LAN を延長して接続することが可能である他、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利用されることもある。

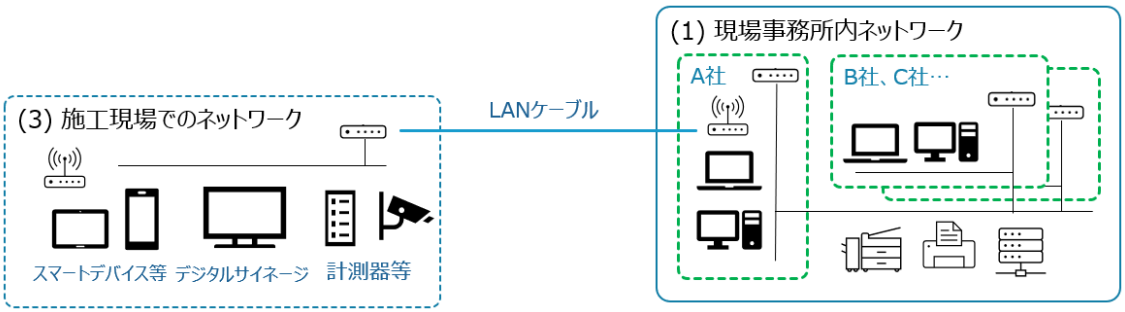

図３－１：LAN ケーブルによる接続

②通信キャリアーが提供する通信回線経由での接続

施工現場と現場事務所が遠距離の場合、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。

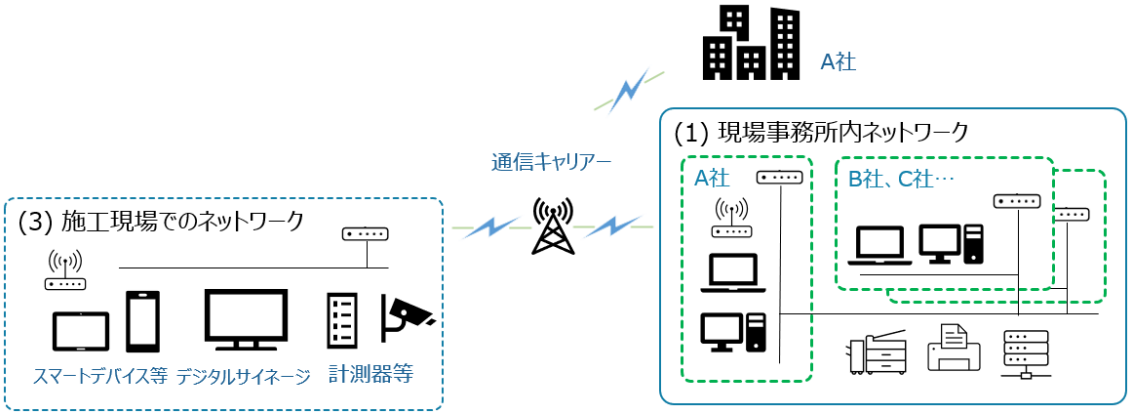

図３－２：通信キャリアーの VPN サービスを利用した接続

③インターネットを利用した接続

通信キャリアーによる 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 で接続可能ではあるが、設定されたパスワードの不備やセキュリティパッチの未適用、製品自身の脆弱性等の問題からサイバー攻撃被害を受ける例が頻発しているため利用は推奨されない。 施工現場 LAN 内に EDR や EPP を導入したセキュリティ対策を施したリモート操作用の PC を設置し、利用者の特定および利用履歴の確認が可能なリモートデスクトップサービスを利用して操作することが望ましい。 また、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。

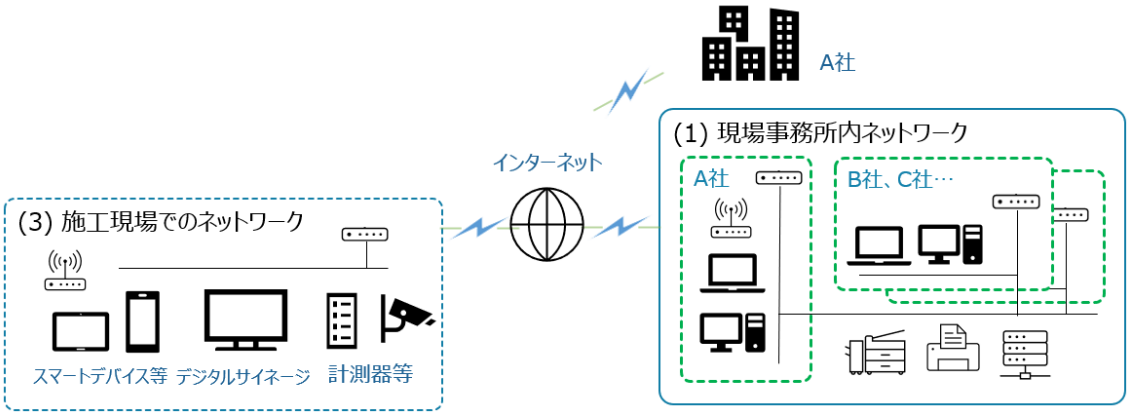

図３－３：インターネットを利用した接続

(2) 施工現場や現場事務所でのスマートデバイスの接続

実施に際しては、「建設現場におけるスマートデバイス利用に関するセキュリティガイドライン」を参照し、 各社の運用方針に従った上で使用すること。

３． ５ 外部関係者のネットワーク

発注者、設計者や、協力会社等の外部関係者と情報共有を行う場合、クラウドサービスの利用が望ましい。 詳細は、「７． 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。

４． 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、ネットワーク図等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。

４． 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。

４． 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) セグメント情報と IP アドレスの管理

セグメント情報・IP アドレスの管理は、各セグメントに付与した 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。

４．３ JV 現場における考慮事項

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。

５．セキュリティ対策

５．１ 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)共有サーバーの配置

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。 共有サーバーの利用時の対策については、「５． ４ クラウドストレージ・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。

５．２　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。

(1) 複数の接続が設定可能

光回線において、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。 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。

(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には、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、マルウェア感染防止、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を監視すること。

５．３　無線 LAN 利用時の対策

無線 LAN は、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・対策例を挙げる。

(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モバイルルーターや Wi-Fi 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・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）

⑤ファームウェアのアップデート

(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・ESSID

③認証情報

④AP の設定時に使用する ID、パスワード

５．４ クラウドストレージ ・共有サーバー（NAS）利用時の対策

(1) クラウドストレージを利用する場合は、最低限 2 段階認証を採用すること。

(2) 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原則個人 ID を発行して利用する。 共有 ID は不正利用等によるセキュリティリスクがある。

(3) 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。

(4) マルウェア対策

共用データのマルウェア感染防止、建設現場ネットワーク全体へのマルウェア感染防止のため、共有サーバーにはマルウェア対策ソフトを導入し、適切な運用を行う。

①マルウェア対策ソフトを導入し、常時稼働させる。

マルウェア対策ソフトは、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マルウェア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。

③OS 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マルウェア対策ソフトが導入できない共有サーバーは、マルウェア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、マルウェア対策ソフトの検索対象にする。

(5) サーバーデータの保護

サーバーの誤操作・故障やマルウェア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。

④ハードディスクの暗号化対策を行う。

(6) 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ハードディスクの暗号化対策を行う。

５．５　スマートデバイス利用時の対策

詳細については、「建設現場におけるスマートデバイス利用に関するセキュリティガイドライン」を参照してください。

URL: https://www.nikkenren.com/publication/detail.html?ci=336

（1）基本的な考え方

①建設現場に持ち込むスマートデバイスにおいて、電話以外の機能（カメラ機能、メール機能、インターネット閲覧機能等）を業務で利用する場合は、現場所長の許可を必要とする。

②現場所長が電話以外の機能での利用を許可する場合は、「４.利用を許可した場合の実施事項」と以下の「禁止事項」を遵守させる。

③施主・事業主からの要求または建設現場特有の事情により、スマートデバイスの建設現場への持ち込みを全面的に禁止するなどの現場特有の事情がある場合は、それに即した利用ルールを策定し遵守させる。

（2）禁止事項

①建設現場で撮影した写真や知りえた情報をＳＮＳ等（ツイッターや LINE、Facebook 等）に投稿することを禁止する。

②スマートデバイスの電話以外の機能（カメラ機能、メール機能、インターネット閲覧機能等）を業務で利用したことによって、スマートデバイス内に保存された工事情報（例えば写真データ）を業務が完了した後も保存し続けることを禁止する。 業務完了後はスマートデバイス内に保存された工事情報を速やかに削除するよう指導すること。

５．６　バックアップ・リカバリー対策

故障やマルウェア感染等により、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。

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、「７．　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。

５．７　IoT 機器の対策（Internet of Things：モノのインターネット）

現場の監視や施工状況の映像共有・作業員の体調管理といった目的のために、ネットワークカメラやデジタルサイネージ・ウェアラブルデバイス等の IoT 機器が、建設現場で多く利用されています。IoT 機器にも情報漏洩やデータの改ざんなどのリスクがあり、その取り扱いには十分に注意をする必要があります。

IoT 機器のセキュリティ対策の詳細については、日建連のパンフレット「IoT（Internet of Things）セキュリティについて」を参照してください。

URL：
https://www.nikkenren.com/kenchiku/ict/security/pdf/about_IoT-Security2.pdf

５．８　建設現場ネットワークのセキュリティ対策

建設現場のセキュリティ対策の詳細については、日建連のガイドライン「建設現場における情報セキュリティガイドライン」を参照してください。

URL：https://www.nikkenren.com/publication/detail.html?ci=337

（1）基本的な対策例

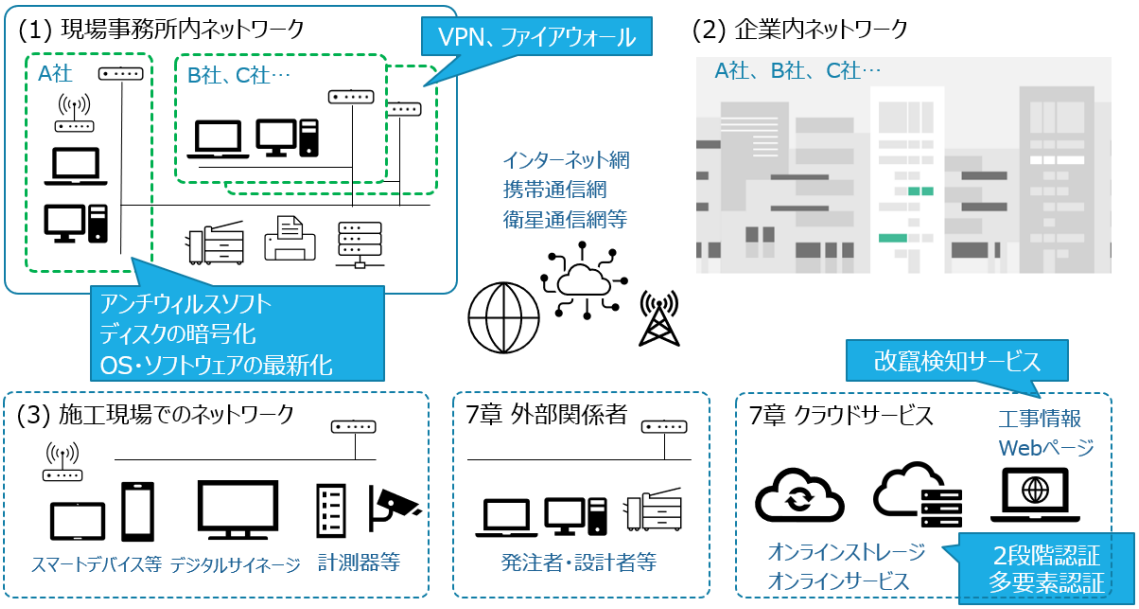

図５：建設現場ネットワークのセキュリティ対策例

（2）高度な対策例

・EDR（Endpoint Detection and Response）：リアルタイムふるまい検知型ウイルス対策

・NGAV（Next Generation Anti-Virus）：AI・機械学習を利用した次世代アンチウィルス

・ASM（Attack Surface Management）：サイバー攻撃の対象となりうる IT 資産を把握し、継続的にリスクの探索・評価を実施する取り組み

・WAF（Web Application Firewall）：Web アプリケーションの脆弱性を突いた攻撃から Web サイトを保護するセキュリティ対策

６．ＪＶ現場ネットワーク構築手順

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を以下に示す。 この手順は参考例であり、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。

手順 1　最初の JV 運営委員会開催時での運営方法の提示

JV スポンサーは、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

②ネットワーク担当者の選定

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覚書の内容： 参考資料：「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）」

本件の詳細事項については、必要に応じて、実務レベルでの会での決定することが望ましい。

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よいか」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に則して運営できる場合は、幹事会社が主導的に、ネットワーク構成ほかの事項を確定する。

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、ネットワーク構成ほかの事項を確定する。

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、運用方法について管理資料を策定し、維持する。

手順 5　覚書の締結

覚書を締結する。

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。

7. 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。

7．1　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。

7．2　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。

７．３　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、マルウェア対策、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。

７．４　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。（パソコンはマルウェア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の対策

２段階認証ないし、多要素認証を利用する。

パスワードの使い廻しをしない。

・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、多要素認証などを利用する。

７．５　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、使ってよい機能など）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。

(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

＜設定例＞

①パスワードは 10 文字以上の英数記号混在とする。

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。

７．６　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。

(1) ストレージサービスの固有の注意事項

①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、を予め決めておく。

②マルウェア対策

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マルウェア対策を実施する。 クラウドサービス側にマルウェア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マルウェア対策を実施すること。

③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。

(2) メッセージングサービスの固有の注意事項

①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。 業務上、必要最低限な機能のみの利用とし、不要な機能が稼動していないか確認しなければならない。

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 ICT 機器が利用されており、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。

執筆委員：最新版（敬称略、五十音順）

遠藤 樹（清水建設）	葛原 徹（大成建設）	上月 章裕（戸田建設）
高馬 洋一（安藤ハザマ）	杉山 宜督（大林組）	仙波 幹徳（三井住友建設）
田口 慶（鹿島建設）	種村 崇（前田建設工業）	豆腐谷 洋一（竹中工務店）
藤井 隆行（東急建設）	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（安藤ハザマ）	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）	

本ガイドライン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・安全環境グループ

〒104-0032 東京都中央区八丁堀 2-5-1 東京建設会館 8 階

TEL:03-3551-1118 FAX：03-3551-4954