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

2016年03月　初版

2024年02月　修正

一般社団法人日本建設業連合会

目　　次

はじめに

昨今、どこでも持ち歩けるスマートデバイスが進化し、建設現場の生産性向上などに役立つツールとして活用が始まっています。しかし、情報漏えい事件・事故の発生源として、スマートフォン・タブレット等（以下、「スマートデバイス」という）に起因するものが拡大しています。スマートデバイスの進展によって、ソーシャル・ネットワーク・サービス（SNS）の特に写真や動画の投稿サイトが手軽に利用できるようになり、機密にすべき情報を安易に投稿して情報漏えい事件や事故が多数発生し、社会問題となっています。これは建設業界も例外ではなく、それに類似した事件・事故の例が見られるようになってきました。言うまでもなく、建設工事を担当するすべての企業がこのような事件・事故を起こさないことが求められています。

このような状況に鑑み、一般社団法人日本建設業連合会は、建設現場における利用を想定した「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」（以下、「本ガイドライン」という）を作成しました。本ガイドラインが、建設業界におけるスマートデバイスの更なる活用と情報セキュリティ事件・事故の未然防止に寄与することを期待するものです。

１．目的

建設現場においては、施工体制が複層化しており、元請のみならず、作業員に至るまで、情報漏えいを起こさないように注意しなければなりません。スマートデバイスは携帯性に優れ、誰でも手軽に利用できる情報機器であることから、作業員が現場にスマートデバイスを持ち込むことを止めることができないのが現状です。このような状況の中で情報漏えいを防ぐため、**「現場所長」**の方に活用していただけるよう、**「情報を守るための基本原則」**に従って本ガイドラインをまとめました。協力会社の社員及び作業員への指導・教育に活用していただければ幸いです。

（情報を守るための基本原則）

（システム＋ルール＋教育＝情報セキュリティ）

①技術的な安全措置:（システム）

攻撃（ウィルス・ハッキング等）を受けて情報資産を奪い取られないように防御するシステム的な手段などを講じておかなければなりません。

②ルール整備

スマートデバイスの持込みや写真撮影の制限ルールなど、情報漏えいリスクを減らす必要があります。

③ 一人一人の適切な行動（教育啓蒙）

ルールや安全措置も、それを利用する作業員がルールを守らなければすべてが水の泡になります。情報漏えいの危険性を理解し、ルールを守るよう、徹底した教育が必要となります。

「建設現場における情報セキュリティガイドラン及び、元請会社における情報セキュリティガイドラインを参照のこと。」

なお、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」に留意してください。

２．対象者と対象物

（１）対象者

建設現場に入場する<u>協力会社の社員及び作業員</u>とする。

（２）対象物

当対象者が建設現場に持ち込む**社有、私有を問わないスマートデバイス**とする。

３．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。

【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。

（工事情報とは）

・図面、工程表、写真、打合せ記録
・発注者、近隣、工事関係者の個人情報（個人の名前が記載された書類等）
・建物の内部や設備の状況（写真等）
・会社の技術やノウハウ（標準仕様等）、管理情報
・その他、施主等から該当現場固有で指定された情報

４．利用を許可した場合の実施事項

（電話以外の機能を利用する場合）

（１）スマートデバイスの利用手続き

現場所長は建設現場に持ち込む機器を特定するため、持込みを行う会社、または、持込みを指示する会社に対して、利用者、利用機器、管理責任者を書面で提出させると共に、情報セキュリティ事故発生時の緊急連絡体制を提出させる。

なお、申請したスマートデバイスの変更や利用者の変更があった場合は、速やかに報告させる。

（２）情報漏えい対策の実施

現場所長は情報漏えい対策として、持ち込まれる機器からの情報漏えいを防止するために下記の対策の実施を求める。なお、私有端末の場合、リモートワイプや業務外アプリ禁止は不可能なため、端末に情報を残さない対策を指導する。

（[文字]は必須項目ではなく必要に応じて実施する項目）

① 盗難・紛失対策

・パスコード／パスワードの設定
・ローカルロックの設定
・常に肌身離さず持ち歩き、置き忘れに注意する。
・[ＭＤＭ等によるリモートワイプ機能]
・[ＰＷを一定回数間違えるとローカルワイプ]

② インターネット接続時の情報漏えい対策

・[セキュリティ対策ソフトの導入]
※Android 端末は必須とする。
・[許可されていないクラウドサービスの利用禁止]
・[許可されたＬＡＮ以外への接続の禁止]

③ その他

・業務に関係のないアプリのインストールを禁止
・管理者の設定したポリシーの変更、機器の改造等を禁止

（３）情報セキュリティ事故発生時の対応

現場所長は、緊急連絡体制に従って速やかに報告させると共に、社内関連部門と連携して事故状況の確認、漏えいデータの把握、お客様報告などを主導・対応する。

５．建設現場での管理方法

（1）利用許可申請

建設現場に持込みを希望する協力会社、または持込みを元請会社から指示された会社の建設現場責任者が、現場所長宛に書面にて利用申請する。

（申請項目の例）

・会社名・所属・住所

・現場代理人名・電話番号・メールアドレス・印

・利用目的・機器利用者名・申請機器　等

（**添付資料−２**「スマートデバイス持込・利用許可申請書」ひな形を参照）

（２）利用許可機器の識別方法

利用を許可した機器は、必要に応じて第三者から利用許可されたことが識別できるようにする。

（識別方法の例）

・利用許可された機器に貼付する「識別シール」を支給する。

・利用許可を示す「ヘルメット用シール」を整備し、許可された利用者に支給する。

・利用許可を示す「あごひも」を整備し、許可された利用者に支給する。

（３）利用誓約

必要に応じて利用者、または持込みを希望する協力会社の現場責任者から誓約書の提出を求める。

（誓約事項の例）

・当該現場におけるスマートデバイス取り扱い規則の遵守

・必要に応じてデバイス内データの開示

・紛失・盗難時の即時報告と遠隔操作による紛失機器の初期化

・業務完了時または当該建設現場離任時に関連業務データの削除

・誓約内容不履行時の罰則受け入れ

（４）機器の管理

機器の紛失・破損を防ぐため、ケースやストラップ（ショルダータイプ含む）を使用し、常に携帯する。

（５）その他

①カメラ利用を禁止する場合

電話機能の利用のために持ち込まれるスマートデバイス対して、カメラ機能の利用禁止を徹底する場合は、「カメラ用セキュリティシール」等を利用する。

②スマートデバイスの持込みを禁止する場合

高いセキュリティレベルを要求される建設現場の場合には、スマートデバイスの持込みを禁止する場合がある。その際には、入退場時の検査の実施、場内の監視カメラ等によるチェック等の方法がある。

添付資料

添付資料−１「情報セキュリティ教育資料（協力会社のみなさんへ)」
添付資料−２「スマートデバイス持込・利用許可申請書」

参考資料

日本建設業連合会のホームページからダウンロードし、利用して下さい。
情報セキュリティに関するガイドライン・教育資料集

https://www.nikkenren.com/kenchiku/ict/security/guideline.html#a2

以下の掲載例は一部です。多くの資料が掲載されていますので、URL リンクからご確認ください。

掲載ガイドライン例

Ⅰ. 建設現場における情報セキュリティガイドライン
情報セキュリティマネジメントシステムの構築と運用手順、実施すべき事項を例示したもの

Ⅱ．元請会社における情報セキュリティガイドライン
元請会社が確実に実施すべき情報セキュリティ対策をとりまとめたもの

Ⅲ．協力会社における情報セキュリティガイドライン
協力会社が確実に実施すべき情報セキュリティ対策をとりまとめたもの

Ⅳ．建設現場ネットワークの構築と運用ガイドライン
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、維持管理方法について解説

掲載教育資料例

パンフレット
・二重脅迫型ランサムウェアの予防と対処について

ポスター
・情報セキュリティポスター「そのメール安全ですか？」（英語版あり）
・情報セキュリティポスター「スマホ注意報」（英語版あり）

動画
・今、そこにある危機
建設業界が直面している情報セキュリティの脅威について解説

・情報セキュリティ５大脅威
建設業界の５つの情報セキュリティ脅威について解説
（英語版、字幕版：中国語、インドネシア語、タイ語、ベトナム語）

あとがき

本ガイドラインの編集にあたっては、一般社団法人日本建設業連合会において長年建設業におけるIT利用の研究に携わってこられた方々、情報ネットワークの企画・構築および情報セキュリティの確立に従事されている方々にご協力を仰ぎ、執筆していただきました。

昨今、情報漏えい事件や情報セキュリティ事故の急増により、個人情報や機密情報を含む業務を委託する際の情報管理の重要性に対する意識が高まってきています。それに伴い、建設現場といえども情報セキュリティ対策の実施を求められることが多くなってきており、その建設工事に従事するすべての会社には、その会社規模によらず、好むと好まざるとによらず、情報セキュリティ対策に取り組むことが求められます。

この様な状況に鑑み、本ガイドラインが、建設業界の目指すべき情報セキュリティ対策の指針として活用され、建設現場における情報セキュリティ事故の発生防止に役立つことを期待しています。

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（敬称略、五十音順）

石垣　順史（清水建設）
葛原　徹（大成建設）
仙波　幹徳（三井住友建設）
豆腐谷　洋一（竹中工務店）
平峯　元晴（東急建設）
山口　正志（フジタ）
大塚　暁（鹿島建設）
高馬　洋一（安藤ハザマ）
津久井　啓介（大林組）
長沼　秀明（戸田建設）
藤野　芳徳（前田建設工業）

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
TEL:03-3551-1118 FAX:03-3555-2463