建設現場における
情報セキュリティガイドライン

2008 年 11 月　初版

2020 年 11 月　改訂

一般社団法人 日本建設業連合会

建築生産委員会 IT推進部会

情報セキュリティ専門部会

目　次

１．はじめに

昨今、各種メディアで取り上げられている情報漏えい事件や情報セキュリティ事故の急速な増加は、情報通信分野における技術的進歩に伴う情報セキュリティリスクの増大がその背景にある。これに加え、情報セキュリティリスクが顕在化した場合の影響を企業が正しく認識していないため、適切な対策が実施されていないことも、要因のひとつになっている。情報漏えい、コンピュータウィルスの感染、ソフトウェアの不正利用・違法コピーなど、情報セキュリティ事故を発生させた企業は、被害者に対する損害賠償の負担だけでなく、「情報化社会に適用できない企業」というレッテルを貼られ、社会的な信用を失墜し、企業の事業活動そのものにも大きな負の影響を受けることになる。

今や、あらゆる組織において、業務と一体化した情報セキュリティ管理の仕組みが必要になっており、業務遂行上どのような情報セキュリティリスクが存在するのかを理解した上で、情報セキュリティ対策を実行していくことが求められているのである。

このような状況を鑑み、一般社団法人 日本建設業連合会は、他産業にはない建設業特有の生産拠点である建設現場に焦点をあて、「建設現場における情報セキュリティガイドライン」(以下「本ガイドライン」という)を作成した。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、建設業各社の建設現場における情報セキュリティ事故発生防止に寄与することを期待している。

１．１　何故、「建設現場の情報セキュリティガイドライン」が必要なのか

(1)IT の導入活用拡大に伴う情報セキュリティリスクの増大

建設現場においても IT の導入活用はますます拡大しており、パソコンをはじめとする IT 機器は業務で不可欠な存在となっている。現場事務所で作成される発注者および社内向けの報告書類や事業所での管理資料は、文書作成ソフト・表計算ソフト・図面作成ソフト(CAD)などのソフトウェアを使用して作成している。発注者・協力会社・社内との情報交換ではメールを利用し、天気や地図など何かを調べようとする場合はインターネットを活用している。会社の業務システムやデジタルカメラによる建設現場の撮影・保存なども日常的に行なわれており、IT は業務に密接なツールとなっている。

一方、IT の普及により情報漏えい、コンピュータウィルスの感染、ソフトウェアの不正利用・違法コピーなどの情報セキュリティリスクも増大している。例えば、情報漏えいに関しては、インターネットの普及、ウィニーなどのファイル共有ソフトに介在するウィルス、記憶媒体(USB メモリ、DVD、CD など)の大容量化が被害を増加させる一因となっている。インターネットが普及する以前は情報を広く流布する手段が限られていたが、インターネットが普及した今日では、不特定多数に簡単に情報発信ができるようになり、インターネットによる情報漏えい被害は増加の一途をたどっている。また、記憶媒体もフロッピーディスクなどの小容量の記憶媒体しかなかった時期は、外に持ち出せるデータ容量も限定されていたが、大容量の記憶媒体の出現により漏えいにつながる情報量も大きくなっている。

IT の進歩により、業務の効率化を支援する便利なツールが増え、ファイルサーバなどによる情報の共有化が進んでいるが、それと同時進行で情報セキュリティリスクも高まっていることを認識しなければならない。IT を有効に活用していくためには、情報セキュリティ対策を実行することが必要な時代になっているのである。

(2)法的規制や各種ルールの強化に伴う法的リスクの増大

IT に関連した事故・犯罪・トラブルの増大という社会的背景を受け、遅れていた IT に関連した法制度の新設・改正が進められており、法的規制や各種ルールが強化されてきた。

例えば、個人情報保護法(2005 年 4 月 1 日施行)の制定は、情報セキュリティ強化を推進する大きな契機となり、「作業員名簿」等の厳重な管理が求められるなど、個人情報を扱っている建設現場においても身近な問題と感じられるようになった。また、近年、著作物の違法複製物である「海賊版」も多く発生しており、著作権法の罰則が 2007 年 7 月 1 日より改正された。具体的には、「10 年以下の懲役若しくは 1,000 万円以下の罰金、またはこの併科」(著作権法第 119 条)に、また、企業などの法人等による侵害の場合も、「3 億円以下の罰金」刑(著作権法第 124 条)が科せられるよう罰則が強化された。

IT に関連する法やルールに背く利用を行った場合は、利用者個人だけでなく法人に対しても罰則規定が適用される場合もあり、個人および企業が社会的制裁を受けることになる。IT を利用する上では、これらの法やルールの遵守が必要となっているのである。

(3)建設現場の特殊性に起因する情報セキュリティ対策上の制約

建設現場においては、IT 技術の積極的な活用や情報共有の拡大・推進により、生産性を向上させる動きが広がりつつあり、CI-NET(建設産業情報化ネットワーク) や電子マニュフェストの利用は、その一例である。この動きをさらに発展させるためには、信頼性の高い IT 活用環境を構築する必要があり、建設現場における情報セキュリティ対策の実施は不可欠である。

しかし、建設現場は、一般的なオフィスとは異なる建設現場固有の下記のような条件があり、情報セキュリティ対策を実施していくには、現場所長をはじめとする全ての職員により一層の負担を強いられるのが実情である。

①建設工事による生産物は単品・個別生産であるため、用途・構造・規模・工法などの各種条件が異なり、すべての建設現場に適用できる作業やルールの標準化がしにくい。

②建設現場は工事期間という有期の利用を前提とした仮設仕様であるため、IT 設備も柔軟に変更や撤去が可能な簡易なものを利用する。(恒久的なオフィスで常設する設備が建設現場では常設しにくい)

③現場事務所の設置・運営費用は現場経費となるため、投入できる費用には大きな制約がある。さらに工期途中で現場事務所を移転・増減する場合は、物理的・時間的・費用的な制約はより一層大きくなる。

④建設現場には元請施工者だけでなく、発注者や設計者、協力会社や資機材メーカー担当

者等、多くの関係者が出入りするうえ、工事の進捗情況により関係者が入れ替わっていくため、一般オフィスよりも情報漏えいのリスクが大きく、情報セキュリティ教育の浸透に手間がかかる。

⑤環境面では、埃が多く、電源も仮設電源を使用するため、情報機器の安定稼動が確保しにくい。図面や書類等は日々変更の連続であるため、原本や最新版の管理における負担が大きい。

このように特殊性のある建設現場を取り巻く環境を正しく認識し、適切な情報セキュリティ対策を実施するには、情報セキュリティ水準の設定とその具体的実現方法に関するガイドラインを示すことが有効であり、本ガイドラインを作成するに至った。

なお、作成に当たっては、ISMS(情報セキュリティマネジメントシステム) フレームワークの考え方を参考にしている。

１．２　本ガイドラインの利用の仕方

(1)利用対象者について

本ガイドラインの利用対象者は、各企業における情報セキュリティ体制の構築担当者、各建設現場における情報セキュリティ対策を実施すべき現場所長または実施責任者である。

(2)利用方法について

本ガイドラインの第２章では、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について述べており、第３章では実施すべき事項を分かり易く具体的に例示した。

まずは、第２章を参考に各企業において、情報セキュリティを推進・運用するための管理体制を構築し、次に第３章を参考にして具体的な情報セキュリティ対策を実施していただきたい。

(3)展開と個別対応について

本ガイドラインは、建設現場において実施される情報セキュリティ対策の方向付けとして、建設業界全体に広く呼びかけるものである。しかしながら、個々の建設現場においては固有の条件が存在することに加え、発注者との合意が優先するため、各建設現場の状況に応じて、本ガイドラインに示す情報セキュリティ対策を取捨選択して適用したり、追加の対策を実施したりする等の適宜対応が必要である。

なお、本ガイドラインにおける情報機器の対象は主にパソコンを想定しており、スマートデバイスのセキュリティ上の取り扱いについては、別途定める「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」を参照いただきたい。

また、特にネットワーク利用上のセキュリティ対策については、別途定める「建設現場ネットワークの構築と運用ガイドライン」の「4. セキュリティ対策」を併せて参照され

たい。

（4）権利関係について

著作権および関係するすべての権利は、一般社団法人 日本建設業連合会に帰属し、本ガイドラインに含まれる著作物の使用(閲覧・複製・引用・配布・印刷)を以下の条件で許可する。

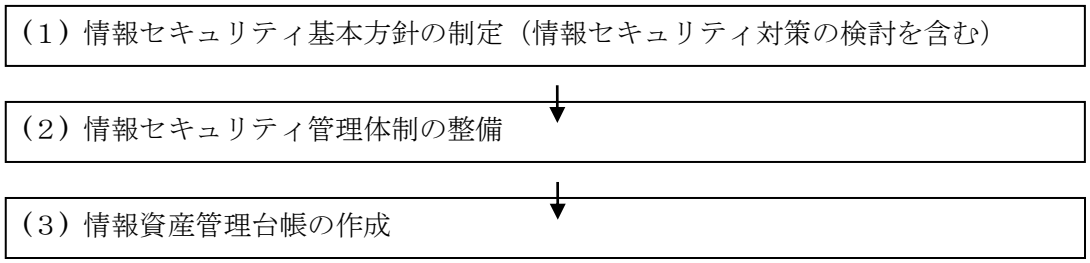
使用条件：１.情報セキュリティ啓発の目的での使用に限ること
２.営利目的ではない使用に限ること
３.複製・引用・配布に際しては、出典を明らかにすること

２．建設現場の情報セキュリティマネジメントシステムの構築と運用の手順

２．１　情報セキュリティマネジメントシステムの構築

情報セキュリティを維持するために、「情報セキュリティ基本方針」を制定し、情報セキュリティ管理体制を整備し、情報資産を調査･分類して情報資産管理台帳を作成する。ここで構築された体制が「情報セキュリティマネジメントシステム」となる。

下図に情報セキュリティマネジメントシステム構築におけるフローを示す。



(1)情報セキュリティ基本方針の制定

「情報セキュリティ基本方針」は、建設現場が情報セキュリティをどうとらえているか、情報セキュリティ維持への取り組みをどのように行っていくかを宣言する公開文書である。また、情報セキュリティ維持を情報セキュリティマネジメントとして、建設現場運営課題の一環として取り組むことを表明する文書でもある。そのため、文章は分かり易くインパクトのあるものが望ましい。

①情報セキュリティ基本方針の制定

現場所長は「情報セキュリティ基本方針」(参考資料－1 に一例を示す)を制定し、情報セキュリティ対策として各項目の具体的な手順やルールを定め、協力会社を含めた現場構成員に周知する。

定期的に手順・ルールの見直しを行い、変更した場合はその都度、現場構成員に周知する。

②JV 現場時の制定方法

JV 現場においては構成会社毎の情報セキュリティマネジメントシステムが異なるため、状況に応じ以下の対応とする。

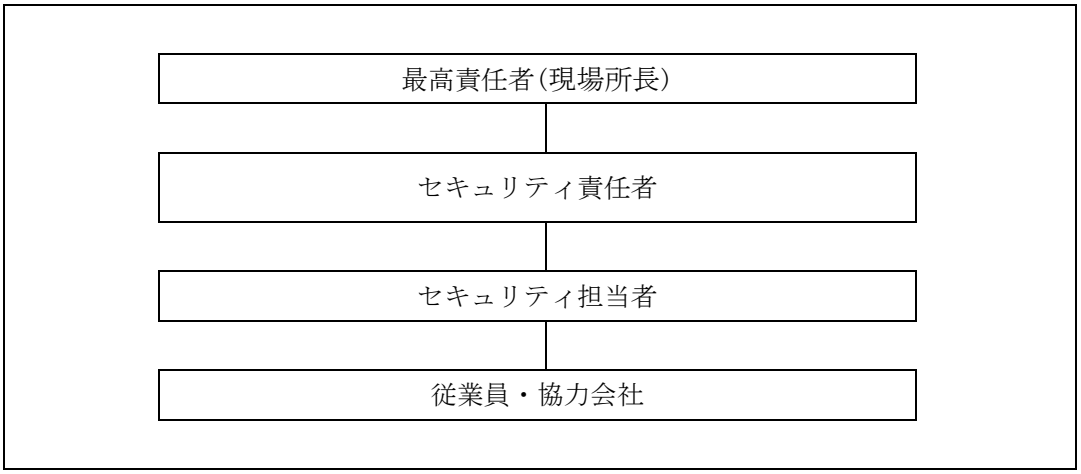
- スポンサー会社に基本方針が設定されている場合は、スポンサー会社の基本方針を用いる。この基本方針に異議等がある場合は、JV 協議会等にて調整する。
- スポンサー会社に基本方針が設定されていない場合は、本ガイドラインの基本方針(例)をベースとしてスポンサー会社が中心となって JV 構成会社と調整し、基本方針を策定する。

(2)情報セキュリティ管理体制の整備

①情報セキュリティ管理体制

建設現場の情報セキュリティ管理体制は、現場内の最高責任者である現場所長と現場所長が任命するセキュリティ責任者、セキュリティ担当者、およびその他現場の管理下で業務に従事する者で構成される。

なお、各担当の兼任は可能であるが、最終的な責任は現場所長にある。



②最高責任者（現場所長）の役割

・現場内の最高責任者として情報セキュリティの全体責任を負う。
・必要な経営資源(人・物・金)の割り当てを行う。
・セキュリティ責任者、セキュリティ担当者を任命する。
・具体的なルールや手順の明文化を指示する。
・セキュリティ責任者から遵守状況を把握し、改善指示を行う。

③セキュリティ責任者の役割

・情報セキュリティに関する具体的なルール、手順を明文化し開示する。
・情報セキュリティに関するルール、手順の教育および周知徹底を行う。
・定期的に遵守状況をチェックし､問題点や不備が発見された場合は必要な改善を行う。

④セキュリティ担当者の役割

・セキュリティ責任者を補佐し、セキュリティ責任者の指示に従って作業を実施する。

⑤JV 現場時の管理体制

・最高責任者はスポンサー会社の現場所長とする。
・セキュリティ責任者は現場所長が任命する者(基本はスポンサー会社)とする。
・セキュリティ担当者は JV 各社より１名任命する。
・セキュリティ担当者は各社間の調整、各社内のセキュリティ確保、各社の本社との調整を行う。

（3）情報資産管理台帳の作成

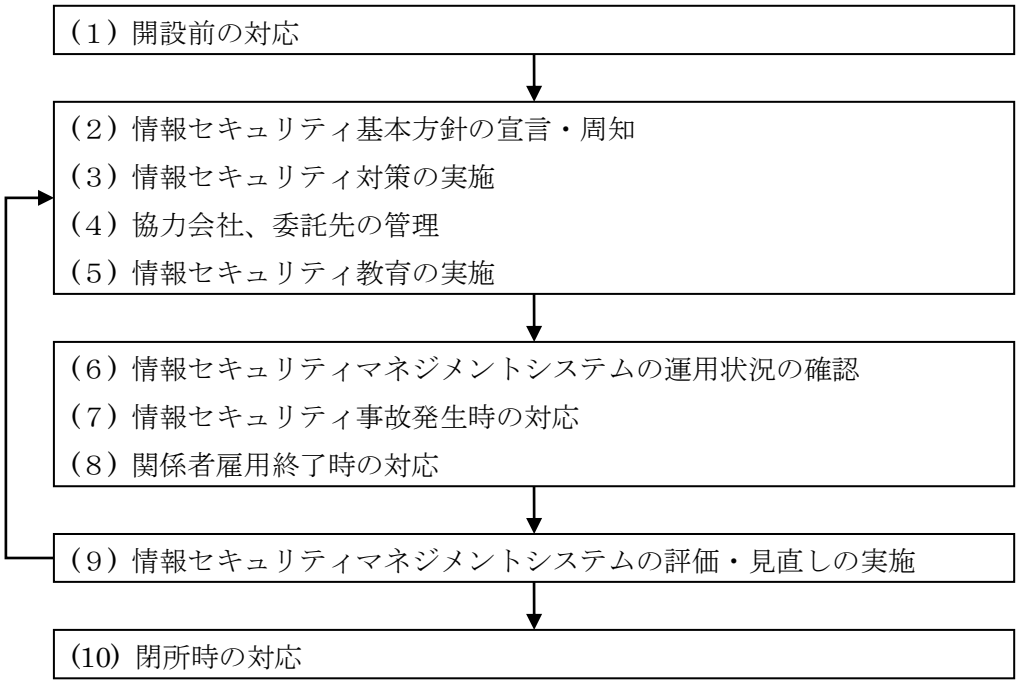
情報資産管理台帳として整備する情報資産とは、建設現場で業務上取り扱う業務情報全般、顧客や関係者の個人情報や情報を処理するパソコン・プリンタなどの情報機器全般を指す。これらの情報資産を洗い出し、情報資産毎に重要度を判断し、管理者・保管場所・閉所時の取扱い等を決定し、情報資産管理台帳として整備する。参考資料－２に情報資産管理台帳の一例を示す。

重要度の判定は、情報資産ごとに下表の３段階に分類し重要度に応じた取扱いを規定化し運用を行う。参考資料－２に情報分類ごとの重要度の例を示すが、当然工事案件の個別要件によっても見直しが必要である。さらに、情報分類ごとに分類内個々の情報について判定を行う必要もある。

重要度　小	漏えいした場合、被害が比較的小さい情報資産
重要度　中	漏えいした場合、信用問題など大きな影響を受ける可能性のある情報資産
重要度　大	漏えいした場合、組織の存続にも影響を及ぼしかねない可能性のある情報資産

２．２　情報セキュリティマネジメントシステムの運用

構築された「情報セキュリティマネジメントシステム」を下図のフローで運用を行い、情報セキュリティの維持･改善を図る。情報セキュリティ対策の実効性を確保していくためには、定期的に運用状況の確認・改善を行っていくことが必要である。



（1）開設前の対応

現場事務所開設前には、当該現場で要求される情報セキュリティレベルを勘案して下記事項を行うことが必要である。

・事務所レイアウトの検討
・保安設備の手配
・ネットワーク回線の手配
・必要な情報機器の手配

（2）情報セキュリティ基本方針の宣言･周知

「２．１情報セキュリティマネジメントシステムの構築」で記載した通り、「情報セキュリティ基本方針」を制定し、宣言・周知する。

（3）情報セキュリティ対策の実施

具体的な実施方法については「３．情報セキュリティ対策の実施」で対策例を示しなが

ら解説する。

（4）協力会社、委託先の管理

・セキュリティ責任者は、協力会社・委託先が情報セキュリティ基本方針に基づき、情報セキュリティに関する具体的なルールや手順を遵守できるかのチェックを行う。
・基準を満たしていない場合は、改善要求し対応状況を確認する。
・現場所長またはセキュリティ責任者は、発注者と締結した契約書の秘密保持や情報セキュリティ関連事項を確認し、その内容を協力会社との下請負契約または委託先との業務委託契約の特記事項、条件書などに明記して契約を締結する。

（5）情報セキュリティ教育の実施

セキュリティ責任者は、関係者全員に情報セキュリティ教育を年１回以上の頻度で実施する。

主な教育内容

・(各社の)情報セキュリティポリシー概要
・建設現場でのセキュリティの必要性
・現場事務所のルール、手順
・情報セキュリティ事故の対応方法と再発防止策
・利用者が行うこと、行ってはいけないこと

（6）情報セキュリティマネジメントシステムの運用状況の確認

・日常的に情報セキュリティマネジメントシステムの運用状況の確認を行う。

（7）情報セキュリティ事故発生時の対応

①管理体制

・関係者は情報セキュリティ事故が発生(可能性がある場合を含む)した場合、各社(JVの場合はスポンサー会社)で定められた連絡網に従って、速やかに現場所長またはセキュリティ責任者に報告する。
・現場所長は本社等の関連部門へ連絡を行う。

報告内容の一例

・発見者の氏名
・発見の経緯
・発見日時、場所
・事故の内容
・情報漏えいの場合、その情報の内容（重要度）

②原因調査と分析

・現場所長またはセキュリティ責任者は、情報セキュリティ事故を調査し、原因を究明

し、再発防止策を立案する。IT 面で専門的な知識を必要とする場合は、本社等の関連部門へ支援を要請する。

・現場所長は、再発防止策の進捗管理を図り、本社等の関連部門へ報告を行う。

③再発防止策の周知

・現場所長またはセキュリティ責任者は、情報セキュリティ事故の原因と再発防止策を現場関係者全員に周知する。

（8）関係者雇用終了時の対応

セキュリティ責任者は、関係者の雇用を終了する場合、以下の作業を実施する。

・アクセス権の削除

・貸与したパソコン、媒体などの返却

・パソコンを持出す場合は、当該現場関係データを削除

・秘密契約継続の確認

（9）情報セキュリティマネジメントシステムの評価・見直しの実施

・セキュリティ責任者またはセキュリティ担当者は定期的(年１回以上)に情報セキュリティマネジメントシステムのチェックを実施し、結果を現場所長に報告する。

・現場所長は遵守状況の適否を判断し、問題があれば改善策をセキュリティ責任者に指示する。

・セキュリティ責任者は改善の進捗や結果を現場所長に報告する。

・チェック結果は記録に残す。

（１０）閉所時の対応

現場事務所は通常の事務所とは違い「有期」という特徴がある。現場終了時をあらかじめ想定した取組みが必要となる。

具体的には、個別の情報資産について閉所時の取扱い状況(廃棄・返却等)を確認のうえ「情報資産管理台帳」に明記し、閉所後の情報漏えいの発生がないようにする。

（１１）JV 現場時の留意事項

JV 協議会等において､本ガイドラインを参考にして情報セキュリティ全般についての取り決めを行い、関係各社了解のうえで現場運営を行う。また、「JV 現場ネットワークの構築と運用ガイドライン」に則ったネットワーク構成および情報セキュリティ対策を実施する。特に下記事項には留意する必要がある。

①他の JV 構成会社固有データの盗用・破壊・改ざんの禁止

②JV 内固有情報の不正使用の禁止

③他の JV 構成会社ネットワークへの侵入の禁止

３．情報セキュリティ対策の実施

本章では、建設現場における情報セキュリティ対策の実施にあたり、各社で具体化を検討される際の参考として対策例を挙げる。

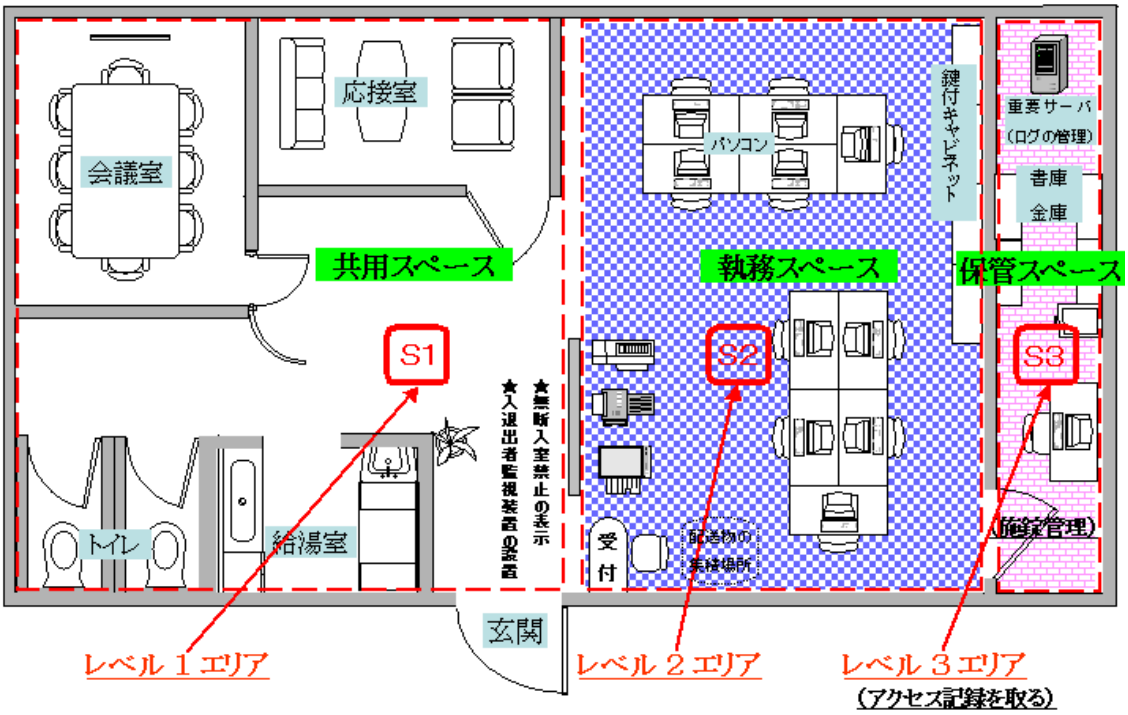
３．１　現場事務所のエリア分類と情報セキュリティ対策

現場事務所内は、必要な情報セキュリティレベルによって分類し、それに応じた対策を実施する。

■情報セキュリティエリアの分類（例）

	分類	必要な対策	例
レベル１エリア	入室（館）の抑止機能があり、かつ無断入室（館）禁止表示等により、第３者の立ち入りが制限されているエリア。	利用目的を明確にする。エリア出入り口に無断入室禁止等の表示を行う。	現場事務所内の共有スペース、会議室、応接室等。
レベル２エリア	従業員以外の出入りが禁止されているエリア。もしくは常時施錠されたキャビネット・引き出し等。	部屋の場合は、原則的に常時施錠する。専用の部屋でない場合は、必ずパーティションなどで区分けをし、従業員が常駐・監視して、従業員以外の出入りを禁止する。キャビネット・引き出しの場合は常時施錠する。	従業員の執務スペースや、施錠されたキャビネット・引き出し等。
レベル３エリア	アクセス権限が規定され、かつ許可された者以外が利用する場合はアクセス記録が取られている常時施錠のエリア、書庫・金庫等。	入室する者が限定された部屋では、常時施錠し、その鍵は特定の個人が管理する。限定された者以外が入室する場合はアクセス記録を取る。書庫・金庫の場合も常時施錠し、その鍵は特定の個人が管理する。	施錠された所長室や、書庫・金庫等。

■エリア例



３．２　情報資産の管理

（１）情報資産の分類と分類に応じた取扱い

情報セキュリティ責任者は、「２．１情報セキュリティマネジメントシステムの構築」の「(３)情報資産管理台帳の作成」で定めた情報資産の評価分類に応じて、各資産の管理責任者を設定し、重要度別に適切なエリアで維持管理を行う。

・重要度小の情報資産は、情報セキュリティレベル１以上のエリアに保管・保存する。
・重要度中の情報資産は、情報セキュリティレベル２以上のエリアに保管・保存する。
・重要度大の情報資産は、情報セキュリティレベル３以上のエリアに保管・保存する。

（２）情報資産の廃棄と再利用

現場事務所内のパソコンや共用のパソコン等情報機器を廃棄または再利用する場合は、その重要度に合わせた管理策を定めこれを実施する。また、情報機器によって作成・印刷された文書等についても、その保存期間を明示するなどの管理策を定めこれを実施する。

■対策例

・情報機器を廃棄する際は、機器(ハードディスクドライブ)を物理的に破壊する。
・情報機器を再利用する際は、データ消去の専用ソフトウェアを使用する。

・文書を廃棄する際はシュレッダ等を用い、情報漏えいを防止する。
・情報漏えいに対して確実な情報セキュリティ対策を講じている信頼性の高い会社に依頼して廃棄を行なう。この場合には、守秘義務等の必要な情報セキュリティ関連要求事項を含んだ契約を締結するとともに、廃棄証明を取得する。

（3）配送物管理

現場事務所からの送付物、現場事務所への配送物に関する管理策を定め、これを実施する。

■対策例

・配送物の集積場所は、常に従業員の目が届く場所とする。
・配送業者との受け渡しにおいては担当者が立会い、授受の記録をつける。
・配送されてきた物に関しては、その場で本人に手渡しする。本人不在の場合は、机等に放置せず、担当者が保管する。

（4）デジタル情報出力時の管理

FAX やプリンタ利用時は、情報流出防止のためのルールを定め、これを実施する。

■対策例

①FAX 利用時

・誤送信の防止策として、送信前に再度相手先番号の確認を行う。特に重要な情報の送信の場合は、複数名で確認し合う。
・短縮番号等を利用する。ただし、相手先番号が変更されていないか等の定期的なチェックを行う。
・送受信紙を FAX 上に放置しない。送信が終了するまで立会い、確認する。送信が完了したらすぐに片付ける。
・FAX 受信については、定められた担当者が受信文書を速やかに本人へ手渡しする。本人不在の場合は、担当者が保管する。

②プリンタ利用時

・プリンタは、出力文書の重要度に応じて設置する情報セキュリティエリアを決定し管理する。重要度の高い場合、ID カード等による認証出力機能つきプリンタの設置も検討する。
・プリンタから出力した用紙は、速やかに回収する。
・近くにシュレッダを設置し、試し印刷など不要用紙をその場で廃棄できる環境とする。

（5）現場事務所外での情報の取扱い

現場事務所外での情報の取扱いに関しては原則禁止とするが、業務上やむを得ず自宅等での業務を許可する場合は、その取扱いルールを定め、これに沿った管理を行う。

■対策例

・現場事務所外での作業を行うときは、その上司および情報セキュリティ責任者の許可を得なければならない。

・取扱う情報機器は、会社貸与機以外の使用は禁止する。

・外部からの現場事務所内ネットワークへの接続は、通信の暗号化および認証機能を利用して実施する。

・特に離席時の情報セキュリティ管理はスクリーンロック等の対策を講じ、家族や業務に関係のない者がアクセスできないようにする。

・情報機器の持出しに関しては、「３．３．１ 情報機器の運用管理」の「(３)情報機器の持出し管理」を参照。

（６）関係者間での情報共有

現場事務所は、発注者や設計・監理者、協力会社等の社外関係者とデジタルデータ等の情報共有(情報のやり取り)を行う場面が多い。その際の情報漏えいに十分留意し、取扱いルールを定め、これに沿った管理を行う。

■対策例

・持ち出し可能な記憶媒体は原則利用しない。利用する場合は指紋認証、データの暗号化等の情報セキュリティ対策を行なう。

・電子メールにて情報のやり取りをする場合は、デジタルデータにパスワードロックをかける。また送信宛先の間違いやデータの添付ミスがない様、十分留意する。重要データを取り扱う場合は、複数人で管理する。

・クラウドサービスの利用については、取扱いルールを定め、これに沿った管理を行う。

(参考「建設現場ネットワークの構築と運用ガイドライン」第２版)

（７）従業員の識別と鍵の管理

従業員を一目で識別できるような方策を講じる。また、現場事務所内エリアの鍵は適切に管理し、紛失時の対策も講じる。

■対策例

・現場内では制服を着用する。また、胸に社員証や名札を付けることを義務付ける。

・鍵は、複数従業員の目の届くところにキーボックス等を設置し、格納する。

・特に情報セキュリティレベル３エリアの鍵は担当者を決め厳重に管理する。

・鍵の紛失が生じた場合は速やかに情報セキュリティ責任者に連絡し、早急に鍵の交換を行う。

３．３　情報機器の維持管理

３．３．１　情報機器の運用管理

（１）情報機器の導入・利用時の管理

パソコン等情報機器を導入または利用する場合はそのルールを定め周知する。

■対策例

・情報機器を導入する場合は情報セキュリティ責任者の許可を得る。

・申請および承認の記録は、申請書または台帳等の形式で管理する。

申請書または台帳で管理する項目の例

・申請者

・申請日

・申請内容（パソコンの導入等）

・承認者

・承認日

・情報セキュリティ責任者は、業務上の必要性が認められる場合のみ承認する。また、システム的な情報セキュリティ要件が満たされているかの確認を行う。

・会社貸与機以外の使用は禁止する。

・食事、トイレ、休憩、会議などで席を外す場合や、外出や退社の際には、第３者による不正な操作や盗み見を防止するため、ログアウトする、スクリーンロックを作動させる、電源を落とすなどの対策を実施する。

・重要な情報が格納された電子ファイルには、第３者による情報漏えいを防止するため、パスワードによる開封制限機能や暗号化ソフトによる暗号化を利用するなどの対策を実施する。

（２）情報機器の保護管理

パソコン等情報機器は、盗難・不正持ち出しの防止対策を行い実施する。

■対策例

・パソコン等情報機器は、情報セキュリティレベル２以上のエリアに設置する。特に重要な情報を管理するサーバ等は、情報セキュリティレベル３エリアへの設置が望ましい。

・パソコンおよびサーバ等は、鍵付きのワイヤ等で事務机や床に固定する。

・持出しが容易なノートパソコン等は、利用時以外は鍵のかかる引き出しやキャビネットに格納する。

（３）情報機器の持出し管理

パソコン等情報機器の現場事務所外への持出しは原則禁止とし、やむを得ず持出す必要のある場合はそのルールを定め、これに沿った管理を行う。

■対策例

・情報機器を持出す場合は情報セキュリティ責任者の許可を得る。
・情報セキュリティ責任者は、業務上の必要性が認められる場合のみ承認する。
・申請および承認の記録は、申請書または台帳等の形式で管理する。

申請書または台帳で管理する項目の例

・申請者
・申請日
・持出しが必要な期間
・申請理由と主な保管情報
・主な持出し場所
・承認者
・承認日（却下日）
・持出し終了確認日

・ 情報セキュリティ管理者が遵守すべきルールを定め周知し、持出しを許可された者がこれに沿った管理を行う。

遵守ルールの例

・持出す場合には、常時携帯し、電車の網棚や車中に放置しない。
・盗難、紛失、置き忘れ等に対する注意を払う。
・持出しを行う情報機器や媒体には、必要な情報のみを保管する。
・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を行う。
・飲酒時、または飲酒の可能性がある場合には、持ち運ばない。
・破損を避けるため、梱包やパソコン用のカバンなどを利用して保護する。
・予め許可された接続先以外のネットワークには接続しない。
・他者に貸与しない。
・第３者がのぞき見ることが可能な状況でパソコンを利用しない。
・盗難・紛失が発生した場合、あるいはその可能性が疑われる場合には、速やかに情報セキュリティ責任者に連絡する。

（4）共有サーバの取扱い

現場事務所内に共有サーバを設置する場合は、サーバ管理者を決め、情報セキュリティ対策を行い実施する。

■対策例

・共有サーバは、UPS（無停電電源装置）の導入やミラーリングなどの RAID（データを複数のディスクに分散すること）を必要に応じて利用して、耐障害性の向上を図る。
・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に保管する。

・共有サーバへのアクセスは、必要最低限の担当者に限定する。

利用者を限定するための対策例

JV 別、JV 構成会社別、役職別、協力会社別などのグループに分け、それぞれのグループに付与する権限を「参照」、「登録」、「変更」、「削除」などの単位で区分する。また、それぞれのグループに対して、必要な権限のみを付与する。

・アクセス制御に関わる承認は、情報セキュリティ責任者が行う。

・アクセス制御に関するルールを定め、周知する。

・ユーザ ID は、原則として個人単位に割り当て、共有 ID は利用しない。

・やむを得ず、共有 ID を利用する場合には、共有 ID の利用者および利用期間を台帳等に記録し、利用者が特定可能な状態にする。

・関係者の異動、退職、契約の終了等がある場合には、アクセス権やユーザ ID の変更、削除等の必要な手続きを可能な限り速やかに行う。

（5）取り外し可能な記憶媒体の管理運用

DVD、USB メモリ、SD カード、ポータブルハードディスク等持ち運びのできる記憶媒体の利用は原則禁止とするが、業務上必要なときはそのルールを定め管理する。

■対策例

・持出し可能な記憶媒体を利用するときは、情報セキュリティ責任者の許可を得る。

・情報セキュリティ責任者は、業務上の必要性が認められる場合のみ承認する。

・利用媒体は、会社から貸与されるパスワードロック等のセキュリティ機能付き媒体のみの利用とし、個人のものは利用しない。

・申請および承認の記録は、申請書または台帳等の形式で管理する。

申請書または台帳で管理する項目の例

申請者記入欄：

・申請者

・申請日

・記憶媒体の利用期間

・申請理由と主な保管情報

情報セキュリティ責任者記入欄：

・承認者

・承認日

・保管データの有無に関わらず、記憶媒体の保管場所は施錠するなど適切な管理を行う。

・媒体は、ラベル付けを行うなどの識別管理を行う。

・USB メモリや SD カードなどの繰り返し書き込みが可能な記憶媒体に書き込んだデータは、利用後、速やかにデータを消去する。

・盗難・紛失が発生した場合、あるいはその可能性が疑われる場合には、速やかに情

報セキュリティ責任者に連絡する。
・情報セキュリティ責任者は、記憶媒体の紛失が発生していないかを確認するため、定期的に棚卸しを実施する。

（6）記憶媒体の処分

利用済みの記憶媒体の処分はその重要度に合わせ処分方法をルール化し、これに沿った管理を行う。

■対策例

・データ消去用の専用ソフトウェアを利用する。
・媒体を物理的に破壊してから廃棄する。
・設定を消去（初期化）する。
・情報漏えいに対して確実な情報セキュリティ対策を講じている信頼性の高い会社に依頼して廃棄を行う。この場合には、守秘義務等の必要な情報セキュリティ関連要求事項を含んだ契約を締結するとともに、廃棄証明を取得する。

３．３．２　アクセス制御

（1）パスワードの管理

パソコン利用時のパスワードやデータフォルダ、ファイルのパスワードを必要に応じ設定し、利用するルールを定めこれに沿った管理を行う。

■対策例

・パスワードは定期的な変更を義務付ける。
・共有サーバ上のパスワードは、情報セキュリティ担当者が定期的に変更し、関係者に伝える。

（2）共用機器の取扱い

現場事務所内での共有機器に関する情報セキュリティには特段の注意を払い、設定管理する。

■対策例

・不特定多数が利用する共用パソコンは、CD/DVD 装置や USB 接続口等外部媒体が接続できない機種を選択設置する。
・現場事務所内 LAN 等への接続は、間にルータなどを設置し接続制御を行う。

３．３．３　ウィルス対策

ネットワークに接続されたパソコンがウィルスに感染すると、現場事務所内だけでなく外部関係者や JV を構成している各社の情報システムを停止させてしまう恐れがある。また、ウィルス感染から情報漏えい事故につながることもあり、取引先の信用低下や感染被害、情報漏えい事故による責任を問われることもあるので、ウィルス対策を確実に実

施することが極めて重要である。

ウィルス対策ソフトが導入できないサーバ(例えばNetwork Attached Storage以下NAS)やパソコンに対しては、ウィルスに感染しないよう現場ネットワーク全体で対策を行う。

このように多層的な情報セキュリティ対策を行うことで問題を発生させ難くすることができるため、様々な方法を組み合わせて実施することが望ましい。

■対策例

・現場事務所内のパソコンおよびサーバには、ウィルス対策ソフト(自動更新できる製品)を必ず導入する。

・ウィルス対策ソフトでは、常に最新のパターンファイルおよび検索エンジンを使用する

・メールソフトで、添付ファイルや html メールを自動的に開かないように設定するなど、アプリケーションのセキュリティ機能を利用する。

・知らない人からのメールに限らず、意味の分からない表題のメールは開封しない。

・業務上必要のないホームページは閲覧しない。

・情報セキュリティ担当者は、定期的に各パソコンのパターンファイルの更新が実施されているかチェックする。

・OS や利用ソフトウェアのセキュリティ修正プログラムについても、定期的に適用状況をチェックする。

・外部からのデータを利用する場合は、ウィルス感染がないことを確認し、利用する。

・ウィルス対策ソフトが導入できない NAS 等は、ウィ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、ウィルス対策ソフトの検索対象にする。

３．３．４　ソフトウェアのインストール

現場事務所内の共有サーバや個人利用のパソコンには、各社で規定されているソフトウェア以外のプログラムをインストールすることや使用することは制限する。やむを得ない場合は、情報セキュリティ責任者の了解のもと、セキュリティチェックなどを十分に行いインストール、使用する。

インストールするソフトウェアは、ライセンス違反を起こさないよう正規にライセンスされたものを導入する。

■対策例

・使用ソフトウェアを限定する。

・定められたソフトウェア以外の使用・インストールは禁止する。

・新規ソフトウェアの導入に関しては、情報セキュリティ責任者の許可を得て、情報セキュリティ担当者の指示に従いインストールする。

・ソフトウェアは、正規にライセンスされたものを利用し、違法コピーされたものは

利用しない。

・ウィニーなどのファイル共有ソフトの使用・インストールは禁止する。(安易な利用は、コンピュータウィルスの感染、情報漏えい事故の発生、著作権法違反等の危険をはらんでいる。)

３．３．５　ログ（記録）の管理

(1)ログ（記録）の取得

現場事務所内サーバの正確なログを取得しておくことは、不正アクセスの発見や情報セキュリティ事故が発生した場合の有力な証跡となることがあるので、その記録取得・保管に努める。

■対策例

・現場事務所内の情報共有サーバのログを取得する。

・各社の規定に従い、一定期間ログを保管する。

・ウィルス対策ソフトのウィルス検索記録を取得する。

・情報機器の設定情報を記録保管する。

ネットワーク機器などは、再起動を行うとログが消失する場合があるので機器の管理者と相談のうえ再起動する。

(2)　現場事務所内のパソコンやサーバの内部時計の同期

現場事務所内での記録の正確性向上のために、現場事務所内の全てのパソコン・サーバなどの情報機器に対して、定期的に内部時計の時刻を合わせる。

■対策例

・インターネット時刻設定の出来る機種は、インターネットからの自動設定を行う。

・各社のネットワークにNetwork Time Protocol Server(NTPサーバ)を設置し、そのNTPサーバと時刻の同期を取る。

・自動設定できない機器は、定期的に時刻の確認や時刻合わせを行う。

参考資料　情報セキュリティ基本方針【例】

情報セキュリティ基本方針

私たち建設業に携わる関係者は、建設現場での業務に関連する情報資産を情報漏えい事件や事故などの脅威から守るとともに、社会と発注者の信頼に応えるため、ここに情報セキュリティ基本方針を定める。

1. 私たちは、建設現場での情報の管理にあたり、情報資産のセキュリティ確保を図るための管理体制を構築し、定期的にその見直しを行うとともに必要に応じて改善する。
2. 私たちは、物理的・人的・IT などの各側面からバランスよく情報セキュリティ対策を講じ、情報漏えい等の問題を発生させない予防策を実施するとともに、万一の問題発生に対しても迅速に対応する。
3. 私たちは、情報セキュリティ対策の推進について、運営体制を定め、役割と責任者を明確にする。
4. 私たちは、建設現場事務所職員・協力会社職員、ならびに現場の管理下で業務に従事する者に対して、本基本方針ならびに関連諸規程などの説明や教育を実施し、それに対する違反行為に対しては就業規則または契約に基づき明確な責任を求める。
5. 私たちは、本基本方針ならびに関連諸規程などが周知・実行・維持され、かつ、継続的改善が行なわれることを確実にするため、定期的にチェックを実施し、問題点を明らかにし、これを解決する。

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、さらに社内において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、それぞれの専門分野において執筆していただいた。

今後、建設現場においてはコンピュータネットワーク導入による受発注者間や自社内、協力会社間、また、他業種間での情報共有が増加していくことは明かであり、そのような環境下で作業所の情報セキュリティを如何に確保していくかを、本ガイドラインに記述された内容を基本として整備促進されていくことが望まれる。また、これからのインターネットを中心とするITの目覚しい進歩を考えると、数年先には本ガイドラインの内容も陳腐化してしまっている恐れが十分考えられる。

今後とも先進的なITの調査を継続しつつ、時機に即した建設現場でのISMS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訂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

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

池端 裕之(戸田建設)	太田 忠宏(鹿島建設)	大山 信一(三井住友建設)
河崎 充(大林組)	北沢 孝宗(鹿島建設)	高馬 洋一(間組)
児山 満(前田建設工業)	柴田 耕作(三菱ﾏﾃﾘｱﾙ)	高橋 均(竹中工務店)
田中 雄一(フジタ)	豆腐谷 洋一(竹中工務店)	友枝 幸一(戸田建設)
長谷 芳春(三井住友建設)	平井 明(大成建設)	平野 岳志(ｵﾘｴﾝﾀﾙ白石)
平原 昇(東亜建設工業)	藤野 芳徳(前田建設工業)	松本 善太(清水建設)
宮田 康弘(間組)		

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