元請会社における
情報セキュリティガイドライン

2010年06月　初版

2026年09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 2
1.1　何故、「元請会社編」が必要なのか 2
1.2　本ガイドラインの利用の仕方 3
２．情報セキュリティ管理の考え方 4
2.1　情報漏えいのリスク 4
2.2　元請会社の役割 5
３．元請会社の実施事項 6
3.1　現場開所時の対応 7
3.2　現場稼動中の対応 9
3.3　現場閉所時の対応 16
添付資料について 17
あとがき 18

１．はじめに

1.1　何故、「元請会社編」が必要なのか

安全や品質と同じく、情報セキュリティ対策についても、協力会社に対する管理責任が元請会社にあることは言うまでもなく、発注者等からは、建設現場に関わるすべての協力会社が一体となった対策が求められています。

一方で、建設現場においては、協力会社の範囲も広く、施工体制も複層化しているため、各社で実施されている情報セキュリティ対策は、その内容もレベルも様々です。

建設現場における情報セキュリティを一定水準以上のレベルに保つためには、各社個別の対応ではなく、建設業界全体としての取り組みが必要であるため、その指針となる具体的な対策を本ガイドラインとして示しました。

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、元請会社の現場所長および現場担当者です。

（2）利用方法について

本ガイドラインは、「第 1 版」を補完する内容で、特に協力会社に対する情報セキュリティ対策についての内容としています。

また、別冊「協力会社編（第２版)」は、建設現場の業務に従事する協力会社の経営層および幹部層、または情報セキュリティ管理者を利用対象者とし、協力会社自身が実施する情報セキュリティ対策についての内容としています。

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」に留意すること。

（3）展開と個別対応について

本ガイドラインは、「第１版」及び「協力会社編（第２版)」とあわせて、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す。

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されるため、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対応が必要です。

（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、(社)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権の使用(閲覧・複製・引用・配付・印刷)を以下の条件で許可します。

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・配付に際しては、出典を明らかにすること

２．情報セキュリティ管理の考え方

2.1　情報漏えいのリスク

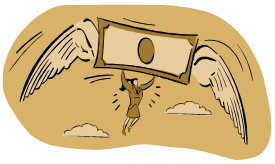
近年、情報漏えいに関する事件・事故がテレビ、新聞等で大きく報道されています。このような事件・事故を未然に防ぐために、情報漏えいのリスクをよく理解して、事件・事故防止に努めて下さい。

（１）もし、情報漏えいが起きたら・・・

個人情報の漏えいなどで高額の賠償金を支払う事例が報道されていますが、建設現場で扱う情報が漏えいした場合も同様のリスクが想定されます。

- 当事者、関係者は厳しく処分される可能性があります。
- 会社の信用を失い、仕事や工事を失う恐れもあります。
- 法律や契約※に抵触し、厳しく責任を問われます。
  - 法による制裁
  - 損害賠償など

※ 個人情報保護法、不正競争防止法、守秘義務契約違反など



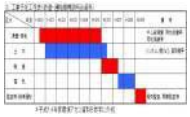


（２）工事に関する「情報」とは？

建設現場で扱われる情報は、下記のように多種・多量に存在します。情報は必ず重要度を把握して、万が一にも情報漏えいが発生しないよう適切に管理･運用を行います。

- 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）
- 関係会社の管理情報











（３）建設現場ではこんな所からも情報が漏れる可能性が・・・

建設現場は協力業者や資機材メーカなど多くの関係者が出入りするうえ関係者の入れ替わりも頻繁で、現場事務所も一般オフィスに比べ情報漏えいリスクが大きいと言えます。そのため思わぬところからの情報漏えいの可能性が考えられます。

- 現場事務所に出入りしていた外部の業者から･･･
- 現場事務所が事務所荒しに遭い、業務用パソコンが盗まれて･･･
- 協力業者まではしっかりとした情報セキュリティ体制だったが、再下請先から･･･
- 現場内の写真をSNSに投稿されて･･･



2.2　元請会社の役割

建設現場は既に述べたようにその特殊性から情報漏えいリスクが大きいですが、万一情報漏えいが発生した場合の損害は一般の情報漏えいとなんら変わりません。元請会社の現場所長は、現場内の情報セキュリティの最高責任者として、情報漏えいの発生がないように現場運営を行う必要があります。

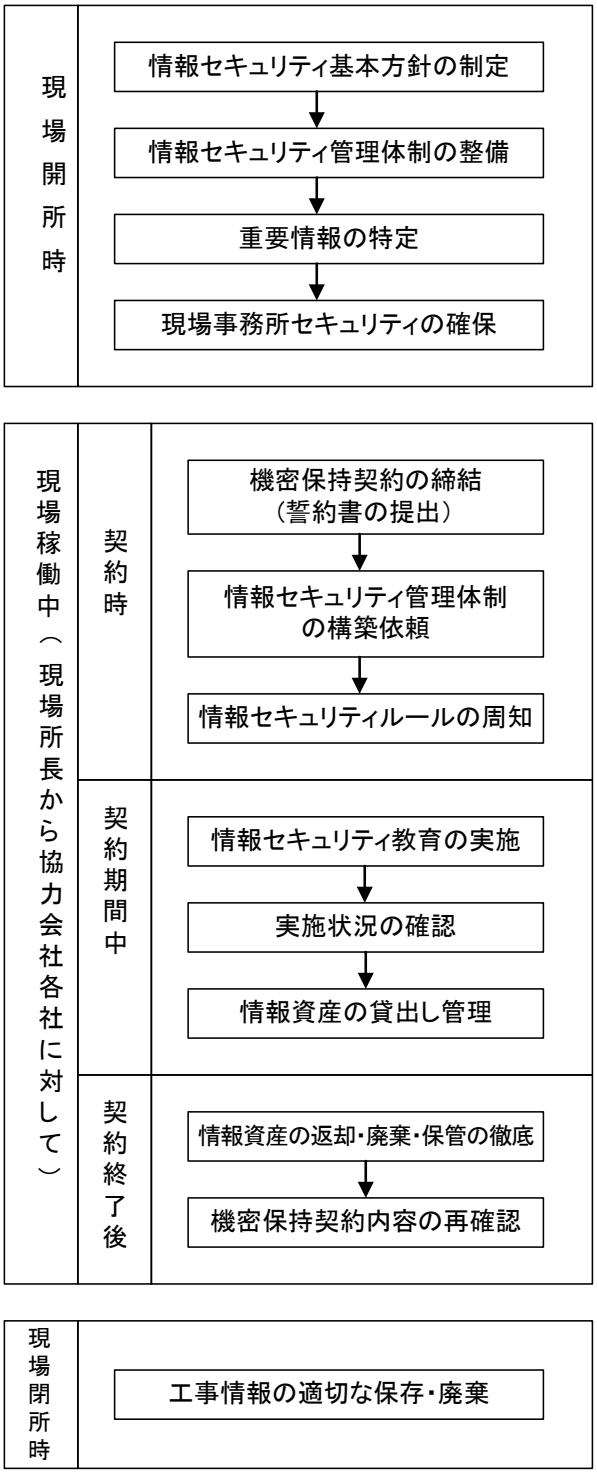
具体的には、第３章の実施事項をよく理解して現場運営に役立てて下さい。

- 現場内の情報セキュリティに関する最高責任者は現場所長です。
- 関係者全体をしっかりと統括していくことが必須です。
- 日々の現場活動の中で日常的に情報セキュリティを管理･運用していく体制の維持が不可欠です。



３．元請会社の実施事項

この章では、現場開所時から現場稼動中、現場閉所時に至る時系列の中で、元請会社が実施すべき事項について説明します。特に、協力会社に対する実施事項については、契約時、契約期間中、契約終了時に分けて注意すべきポイントをあげています。



3.1　現場開所時の対応

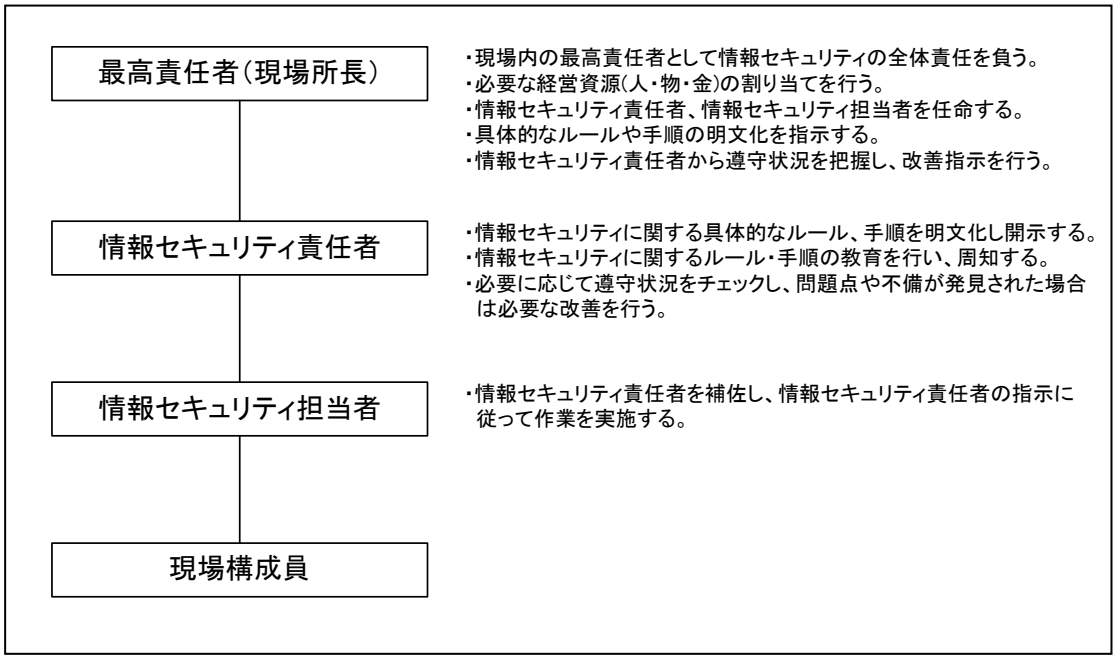
ここでは、現場開所時に元請会社が実施すべき 4 つのポイントについて、「第 1 版」の内容を要約して説明します。

（1） 情報セキュリティ基本方針を制定しましょう

・「情報セキュリティ基本方針」（「第 1 版」参考資料－1)を制定します。
・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ます。
・従業員および協力会社を含めた現場構成員に周知します。
・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ことも必要です。

（2） 情報セキュリティ管理体制を整備しましょう

・情報セキュリティを推進する元請会社の管理体制を組織します。



・建設現場が稼動すると、協力会社に対しても同様に、情報セキュリティ管理体制の構築を依頼します。詳しくは 3.2 で説明します。

（3） 建設現場の重要情報には何があるかを特定しましょう

・2.1 で述べた「工事に関する情報」の洗い出しをします。

・情報ごとに重要度を判断し、管理責任者・保管場所・閉所時の取扱い等を決定します。重要度の判定は、漏えいや喪失した場合の影響度により、以下の 3 段階で判定します。

重要度　小	業務への影響が比較的小さい情報
重要度　中	業務に大きな影響を与える可能性のある情報
重要度　大	事業の存続に大きな影響を与える可能性のある情報

・これらを、情報資産管理台帳として整備します。情報資産管理台帳の一例としては、「第 1 版」参考資料－2 を参照して下さい。

（4） 現場事務所のセキュリティは大丈夫ですか？

現場事務所においても、当該建設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の検討が必要です。

・物理的セキュリティにも配慮した現場事務所レイアウト(「第 1 版」3.1 参照)の検討

・保安設備や保安システムの導入

・現場事務所内ネットワーク構成の検討と回線の手配

・適切な情報機器の手配

3.2　現場稼動中の対応

ここでは、元請会社が協力会社と工事契約する際、契約期間中、契約終了時の対応に関する注意事項について述べます。建設現場には多くの協力会社が出入りし、工事の進捗状況に応じてそれらの協力会社も入れ替わります。対応に不備がないように、十分注意することが必要です。

（１） 契約時の対応

①機密保持契約を必ず締結しましょう

発注者等から当該工事に求められている守秘義務と同等の機密保持契約を、元請会社と協力会社の間で締結します。工事が終了した後も、守秘義務が有効となる内容になっていることが必要です。

契約内容については、工事契約時に協力会社に説明し、理解を得ることが重要です。

＜具体的な実施例＞

協力会社との工事契約書にて、発注者等から当該工事に求められている守秘義務と同等の機密保持についての内容が盛り込まれているか確認します。

盛り込まれていない場合は、協力会社に対し別途、同等の内容を記載した誓約書の提出を求めます。

誓約書は、個別契約ごとに提出を求める場合もありますが、元請会社と協力会社の間で包括して提出を求めることも可能です。

・添付資料－３「誓約書例」



・ 工事契約時には、必ず機密保持契約が含まれているか確認しましょう。
・ もし含まれていなければ、別途、誓約書の提出を求めましょう。

②協力会社に情報セキュリティ管理体制の構築を依頼しましょう

元請会社は協力会社に対し、「情報セキュリティ責任者」と「情報セキュリティ担当者」の選出を依頼します。(協力会社の規模等の事情に応じて、これらの役割を兼任することも可能とします。) 例えるならば、これは“情報についての安全衛生責任者”の選出を求めるようなものです。

協力会社内では、自社についての情報セキュリティ対策を実施します。具体的には、元請会社からの指示事項の伝達･実施･確認、また情報セキュリティに関する問題発生時には元請会社への報告・対処が主な役割となります。

現場全体の情報セキュリティ管理体制を明確にするための有効な手段として、施工体制図に各社の「情報セキュリティ責任者」を併記する方法もあります。



【施工体制図への記載事例】

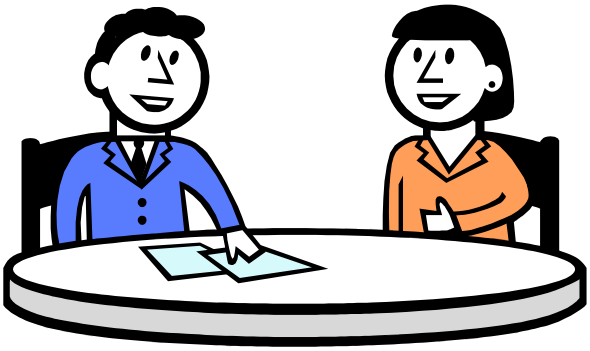
- 協力会社に「情報セキュリティ責任者」と「情報セキュリティ担当者」の選出を依頼しましょう。
- 現場全体の情報セキュリティ管理体制を明確にしましょう。

③情報セキュリティルールを周知しましょう

元請会社が定めた情報セキュリティルールを協力会社に周知します。
協力会社が再下請けする場合には、再下請先に教育、指導することも依頼します。(特に１次協力会社には、送り出し教育時に建設現場の情報セキュリティルールについても指導することを依頼します)

＜具体的な実施例＞

・建設現場の情報資産管理について
（重要情報の授受方法、情報の貸出し方法、複写･複製に関するルール等）
・現場事務所のセキュリティ区画の確認（立入り禁止区域等の確認）
・送り出し教育の実施依頼
・事故発生時の対応



- 協力会社に対し、建設現場の情報セキュリティルールを周知しましょう。
- 特に、再下請先にもルールを周知･指導するよう、依頼しましょう。

（２） 契約期間中の対応

①情報セキュリティ教育を実施しましょう

各社の責任者、作業員および図面等の情報資産を取扱う担当者に対し、情報セキュリティ教育を実施します。

１）新規入場者教育時

情報セキュリティの必要性と最低限守るべきルール、情報セキュリティ事故発生時の対応方法について説明します。

＜具体的な実施例＞

・対象者に対し、添付資料－１「協力会社の皆さんへ　情報漏えい防止徹底のお願い」を配付して説明します。

２）朝礼、定例会議、協議会等

情報セキュリティ意識の向上のため、当該工事の関係者に対し、定期的・継続的に教育を実施します。

＜具体的な実施例＞

・朝礼時に、協力会社作業員に対して「情報セキュリティにおける実施事項」について教育します。（内容は別冊「協力会社編」を参照）

・定例会議、災害防止協議会等の機会をつかって、協力会社に対して情報セキュリティ対策の重要性を説明します。



・ 協力会社に対しあらゆる機会を使って、定期的に建設現場の情報セキュリティ対策の重要性を説明しましょう。

②協力会社の実施状況を確認しましょう

当該工事の業務において、実際に情報セキュリティルールが遵守されているかを必要に応じて確認し、指導します。

＜具体的な実施例＞

・「情報セキュリティパトロール」を定期的に実施し、協力会社の情報セキュリティ責任者が、自社作業員がルールを遵守しているか、確認します。

・添付資料－４「情報セキュリティチェックシート（現場代表者・機器取扱者用）」を協力会社の情報セキュリティ責任者に配付して回答してもらいます。
結果を確認し、必要ならば対策の実施を指導してください。
（最低年に１回は実施が望ましい）

・情報の受け渡し時や貸出し時の機会を通じて、情報セキュリティルールを守っているか、協力会社作業員に確認します。



・ 協力会社作業員が、実際に建設現場の情報セキュリティ対策を実施しているのか、確認しましょう。

③情報資産の貸出し時は注意しましょう

当該工事の業務において、重要な情報資産を協力会社や再下請先へ貸出しを行う場合は、「【重要情報】貸出台帳」等で、適切に管理します。

＜具体的な実施例＞

・添付資料－2「【重要情報】貸出台帳」の利用

・情報セキュリティルールの再確認

【重要情報】貸出台帳

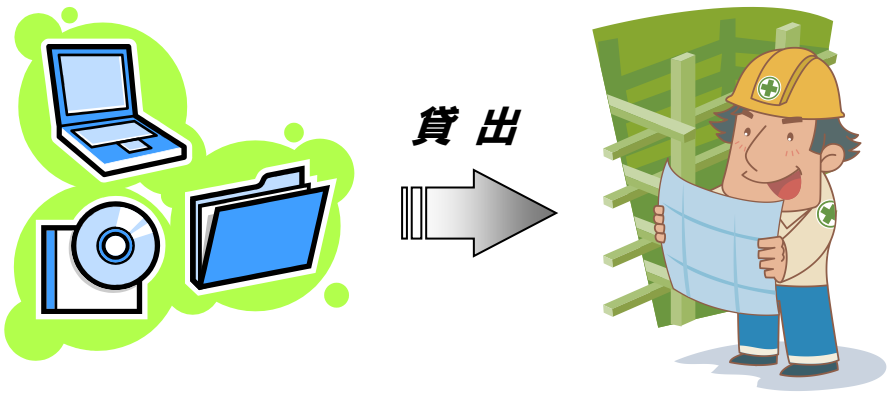
【貸出会社】　ＸＸ建設㈱　ＸＸ作業所　　情報セキュリティ責任者：XX　XX

【預り会社】　ＸＸ工務店　　情報セキュリティ責任者：XX　XX

■ 当台帳は元請・一次会社・二次会社等、工事に係る会社が重要情報を貸し出す場合に必ず記帳・管理する。
■ 当台帳は貸出会社が返却まで管理して、返却後も他の工事関連書類と同様に保存する。
■ 返却が困難な場合は、預り者が責任を持って廃棄・削除して、当台帳は必ず記載する。

（No. 1）

No	資料種別	資 料 名	媒体	数量	貸出時				返却時			
					貸出日	返却期限	貸出者印（XX建設）	預り者印（XX工務店）	返却日	預り者印（XX工務店）	貸出者印（XX建設）	返却方法
1	施工図	XX工事　M階部分図面	書類(紙)	2枚	2010年 4／20	2010年 9／16	㊞	㊞	2010年 9／14	㊞	㊞	2枚返却
2	施工図	XX工事　N階部分図面	書類(紙)	10枚	2010年 5／17	2010年 10／20	㊞	㊞	2010年 10／19	㊞	㊞	廃棄（シュレッダー）
3					／	／			／			
4					／	／			／			
5					／	／			／			
6					／	／			／			
7					／	／			／			
8					／	／			／			

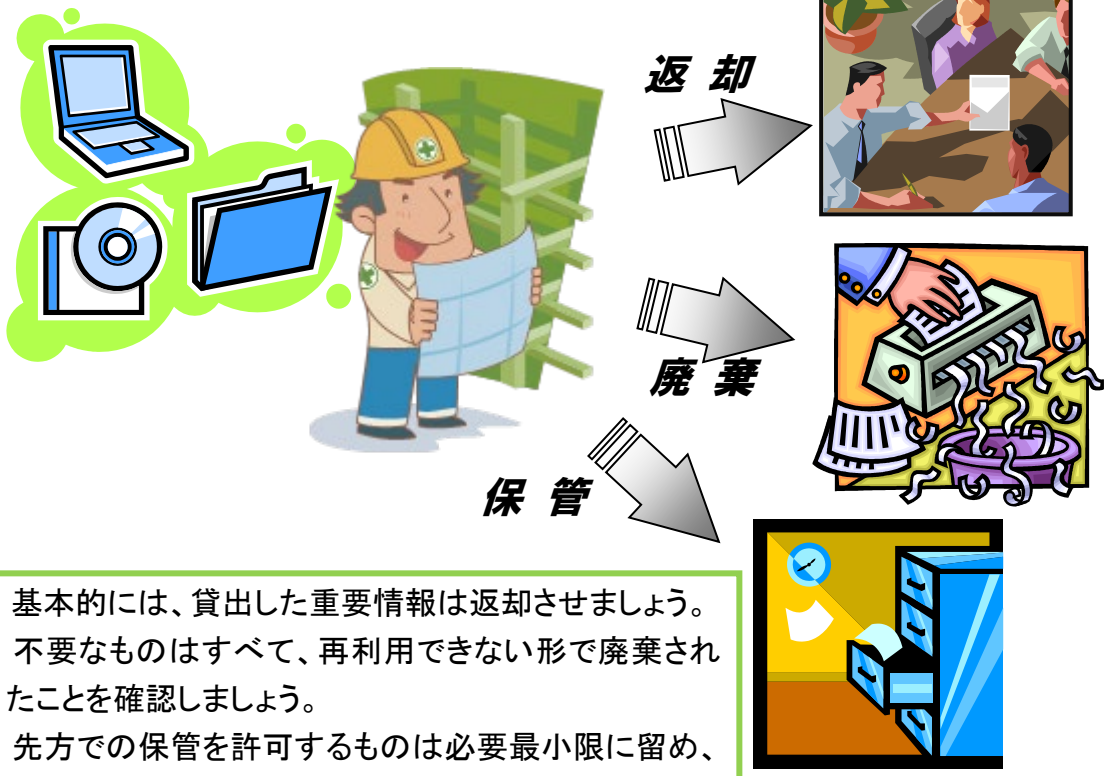


・　どの協力会社にどんな重要情報を提供したのか、正確に把握するとともに、先方での管理者を明確にし、適切に取扱うよう、確認しましょう。

（３） 契約終了時の対応

①情報資産の返却・廃棄・保管を徹底させましょう

協力会社や再下請先に提供している情報資産の有無を確認し、適切に返却・廃棄・保管させます。



- 基本的には、貸出した重要情報は返却させましょう。
- 不要なものはすべて、再利用できない形で廃棄されたことを確認しましょう。
- 先方での保管を許可するものは必要最小限に留め、適切に取扱うよう、指示しましょう。

②機密保持契約内容の再確認

通常、協力会社や再下請先との原契約が終了した後も、機密保持に関する契約事項は有効です。あらためて、その内容や有効期間を確認します。



- 請負契約書や機密保持契約書を見直し、協力会社や再下請先に対し、機密保持に関する契約内容を再度、周知しましょう。

3.3　現場閉所時の対応

現場閉所時においては、記憶媒体が紙か電子的かを問わず、すべての情報について適切に保管・廃棄を行うことが必要です。機密保持契約書や「【重要情報】貸出台帳」等も忘れずに保管してください。また、パソコンやプリンタなどをリース契約している場合は、リース契約機器の返却時に機器内に重要な情報が残存していないかの確認をすることが必要です。



- 重要情報を取扱った記憶媒体の“ポイ捨て”は、厳禁です。
- 紙文書や記憶媒体を廃棄する場合は、破砕、溶解等を行い、判読不能な状態で廃棄しましょう。
- パソコンやプリンタなどを廃棄する場合は、データが残存しないように措置を講じましょう。
- パソコンやプリンタなどをリース会社等へ返却する場合は、返却先にデータ消去を依頼することも可能です。
- クラウドサービスを利用していた場合は、保存されているデータを確実に削除しましょう。

添付資料について

本ガイドラインの添付資料を利用する際は、日本建設業連合会のホームページから、オリジナルファイルをダウンロードしてお使いください。

添付資料－１・「協力会社の皆さんへ　情報漏えい防止のお願い」

添付資料－2・「【重要情報】貸出台帳」

添付資料－3・「情報漏えい防止に関する誓約書」 例

例1・情報漏えい防止に関する誓約書（再下請負通知書対応版）

再下請負通知書に別添となる誓約書例です。

再下請負通知書には、「元請会社（JV）を含む上位の注文者に対し、別添『情報漏えい防止に関する誓約書』の内容を遵守することを誓約します。」の記述が必要です。

例2・情報漏えい防止に関する誓約書（基本契約締結会社用）

新たに基本契約を締結する会社が当社に対し提出する誓約書です。

添付資料－4・「情報セキュリティチェックシート(現場代表者・機器取扱者用)」

【参考】

○**「中小企業の情報セキュリティ対策ガイドライン」**（独立行政法人情報処理推進機構）

https://www.ipa.go.jp/security/guide/sme/about.html

あとがき

情報漏えい事件や情報セキュリティ事故は、これまで以上に増加しており、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。平成22年6月に「建設現場における情報セキュリティガイドライン（元請会社編・協力会社編）」を発行しましたが、さらなるセキュリティ向上に向けて、今回「第２版」として改定しました。

この様な状況を鑑み、本ガイドライン（元請会社編 第２版）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発生防止に役立つことを期待しています。

2015 年 1 月の改定について

ガイドラインの利用者の違いにより、考え方や対応方法等の違いが顕著になってきたため、平成 22 年 6 月に発行した「情報現場における情報セキュリティガイドライン【元請会社編／協力会社編】」を【元請会社編】と【協力会社編】に分割

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

2026 年 9 月の修正について

添付資料内の記載について、技術環境の変化を踏まえ、現在の利用実態および情報セキュリティ要件に即した内容へ改定しました。

執筆委員：最新版（敬称略、五十音順）

有原 淳（前田建設工業）　　石浦 尚樹（フジタ）
石津 理（安藤・間）　　遠藤 樹（清水建設）
上月 章裕（戸田建設）　　岸本 雅彦（奥村組）
葛原 徹（大成建設）　　杉山 宜督（大林組）
仙波 幹徳（三井住友建設）　　豆腐谷 洋一（竹中工務店）
藤井 隆行（東急建設）　　矢口 賢一（鹿島建設）
吉川　遵（五洋建設）

執筆委員：初版

石垣　順史（清水建設）　　葛原　徹（大成建設）
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）　　中俣　一夫（鹿島建設）
長沼　秀明（戸田建設）　　平井　明（大成建設）
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・安全環境グループ
〒104-0032 東京都中央区八丁堀2-8-5 東京建設会館5階
TEL:03-3551-1118 FAX: 03-3551-4954