協力会社における
情報セキュリティ対策について

2010年06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

企業にとっての情報資産（紙媒体・電子データを含む情報及び情報を管理する機器等）とは、蓄積されたノウハウであり、取引先の機密情報であり、お客様や従業員の個人情報です。情報資産は、様々な「脅威」にさらされており、脅威から守るために、「情報セキュリティ対策」が必要となります。

従来、建設業においては図面、パソコン等の紛失や、SNSへの工事写真の投稿など内部関係者の過失によって引き起こされる情報セキュリティ事故が多く、ルールの整備とその教育を通じた人的対策が有効でありました。しかし2016年以降、サイバー攻撃の脅威が高まり、2019年頃からは、企業のネットワークに侵入し機密情報を窃取したのちに、パソコンやファイルサーバーのファイルを暗号化し、暗号化ファイルの復旧と窃取した情報の暴露を止めるための身代金を要求する、二重脅迫型ランサムウェアの被害が増加の一途をたどっています。

本資料は、会員各社が建設現場に従事する協力会社の情報セキュリティ対策の強化を促す際の参考資料としてまとめました。

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の構築に向けて（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」に留意してください。

「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の構築に向けて（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）

２．情報セキュリティ対策とは

この章では、情報セキュリティの概要について解説します。

情報セキュリティ対策とは、まず「守るべき工事情報」を把握し、「情報を守るための基本原則」を理解することから始まります。
情報の扱いは、紙媒体・電子データ共に全く同じです。

（１）守るべき工事情報

① 図面、工程表、写真、打合せ記録
② 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）
③ 建物の内部や設備の状況（写真等）
④ 工事の技術やノウハウ（標準仕様等）
⑤ 関係各社の管理情報

機密情報や個人情報（以下、重要情報という）の取扱いは工事情報の中でも特に細心の注意が必要です。

■機密情報：機密事項と明記された文書や機密であることを前提にした情報
■個人情報：個人を識別できる情報（氏名・性別・年齢・住所・電話番号等）

（２）情報を守るための基本原則

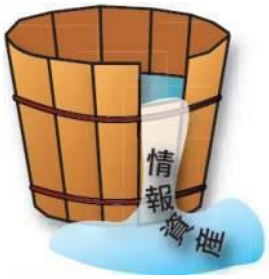
（システム＋ルール＋教育＝情報セキュリティ）

①　外部からの攻撃を防御する（技術的な安全措置：システム）
攻撃（ウイルス・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を講じておかなければなりません。

② 盗難・紛失等によるリスクを減らす（ルール整備）
情報（機器）を社外に持ち出すことを制限・禁止して盗難・紛失の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）
せっかくのルールも安全措置も、それを利用する従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、従業員への徹底した教育が必要となります。

情報セキュリティは、「桶の理論」にたとえられます。一人でもセキュリティ意識、レベルの低い人がいると、そこから情報が漏れるという意味です。全員が同じレベルで、情報セキュリティを保たなければなりません。



３．具体的な情報セキュリティ対策について

重要情報を守り、情報漏えいさせないためには、会社（組織）として情報セキュリティ対策に取り組み、具体的な実施事項を社員および関係者に徹底させることが重要です。

この章では、「3.1 会社の情報セキュリティ対策への取り組み」と「3.2 情報セキュリティにおける実施項目」、および建設業の特色として「3.3 二次以降協力会社への留意事項」について事例をもって紹介します。

3.1　会社の情報セキュリティ対策への取り組み

会社としての情報セキュリティ対策の一例として、事例を交えて以下の４つに整理しました。これらを参考に協力会社へ対策の強化を促してください。

（１）管理体制の構築

（２）具体的な情報セキュリティ施策とルール化

（３）情報セキュリティ教育

（４）情報漏えいなどの事故発生時の対応

（1）管理体制の構築

●経営者が、情報セキュリティ管理体制を構築することが重要

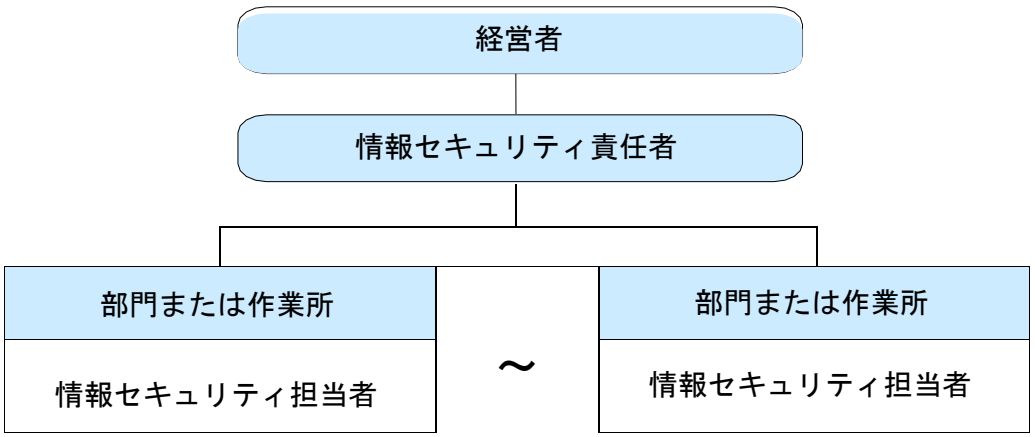
協力会社へは、「経営者がその重要度を理解することが肝心で、その上で情報セキュリティ方針を策定し、推進する組織を作り、人を配置する。また、情報セキュリティ施策の実施状況を適宜確認し、必要に応じて改善していくことが重要である。」ことを説明してください。

具体的事例としては

① 情報セキュリティを管理・推進する組織を構築する。
② 情報セキュリティ責任者・担当者を任命する。
③ 情報セキュリティチェックを定期的（例：年１回以上）に実施する。
④ 社内教育や情報セキュリティ事故に対応できる人材を育成する。

■管理体制と役割（例）

＜管理体制＞



＜役割＞

情報セキュリティ責任者

・情報セキュリティを総合的に管理する。
・情報セキュリティ方針・実施施策を計画・推進する。
・ルール（社内規定等）を策定し、教育する。

情報セキュリティ担当者

・各部門または作業所において、情報セキュリティ施策を実践する。

■定期的な情報セキュリティチェック

情報セキュリティ責任者は、添付資料-１「情報セキュリティチェックシート」を使用して、情報セキュリティ施策の実施状況を確認し、経営者に報告する。チェックシートで明らかになった不備事項については、必要に応じてセキュリティ専門会社等にも相談し、改善策を検討・実施する。

（2）具体的な情報セキュリティ施策とルール化

協力会社には、具体的な情報セキュリティ施策を紹介するとともに、そのルール化と定期的な見直しの重要性についても説明してください。

1）具体的な施策事例

■管理面からの施策事例

① 組織的施策

・情報セキュリティ方針の策定と管理体制の構築

・事件・事故発生の報告ルールと再発防止策の策定、等

② 物理的施策

・パソコンおよびデータ保存用媒体の保護

・パソコンの日常管理（資産管理、盗難・紛失防止、私有情報機器禁止）

・サーバー室等の入退管理

・書類等紙媒体の廃棄（シュレッダー、溶解)、等

③ 人的施策

・社員に対しての情報セキュリティ教育

・社員に対しての機密保持誓約書違反時の罰則規定

・二次以降協力会社等の機密保持誓約書締結と違反時の罰則規定

・二次以降協力会社等への情報セキュリティの注意喚起等

■技術面からの施策事例

① 基本的な施策事例

・パスワードの管理

・ウイルス対策

① パソコン、サーバー、各種ネットワーク機器の基本ソフト（ＯＳ）のセキュリティパッチの適用

② 各種ＯＳやソフトウェアはメーカーサポートされている最新のバージョンを利用

・データの暗号化（ネットワーク上、情報機器内、記憶媒体)

・アクセスログの取得

・業務で使うメールシステムは　Microsoft Officeやビジネス用Gmailなど、ウイルスや迷惑メールを駆除する機能を有する製品・サービスの採用

② ランサムウェアなどのサイバー攻撃を想定した施策

※ 詳細は、日建連の情報セキュリティに関するガイドライン・教育資料集のパンフレット「二重脅迫型ランサムウェアの予防と対処について」を参照ください
https://www.nikkenren.com/kenchiku/ict/security/pdf/2021_security_pamph.pdf

(a) 侵入予防

イ．自社のインターネットの出入口を確認

「SHODAN」等のツールで自社のインターネット出入口の不要なポートが開かれていないかを確認

RDP（ リモートデスクトップ）や インターネットVPN を確認

ロ．出入口のセキュリティ強化

不要なポートを閉じる／制限する／脆弱性を無くす

ハ．本格調査と本格対策

セキュリティ専門会社によるペネトレーション（侵入）テスト

セキュリティ専門会社によるアセスメント・アドバイス

(b) 感染予防

イ．中小企業向け 「サイバーセキュリティお助け隊」制度の活用

・https://www.ipa.go.jp/security/keihatsu/sme/otasuketai/index.html

ロ．EDR（ふるまい検知型ウイルス対策ソフトウェア）の導入

出入口対策やウイルス対策ソフトでも侵入を防止できない最近の
ランサムウェア等の強力なマルウェアが、サーバーやパソコンで
活動することを阻止する。侵入を前提とした最後の砦となるツール。

・ランサムウェアによる暗号化防止

・社内に侵入するためのバックアドアを仕掛けるマルウェアの感染防止

ハ．Windows Active Directory ドメイン管理者の権限管理

・一般ユーザーにローカル管理者権限を与えない

(c) 攻撃への備え

イ．バックアップ取得と復旧訓練

オンラインまたはオフラインバックアップを複数とることが望ましい
定期的な復旧訓練で復旧できることを確認しておくことが必要

ロ．サーバー・ネットワーク機器・パソコン 等の監査ログの取得

ハ．サイバーセキュリティ保険への加入検討

(d) 実際に被害が発生した時の対応

イ．通報・相談・アドバイス

警察（#9110 , https://www.npa.go.jp/cyber/soudan.html）

IPA 情報処理推進機構 情報セキュリティ安心相談窓口
（https://www.ipa.go.jp/security/anshin/）

JPCERT：Japan Computer Emergency Response Team Coordination Center
（info@jpcert.or.jp , https://www.jpcert.or.jp/incidentcall/）

ロ．専門会社へ調査・対処の依頼

サイバーセキュリティ事故 緊急対応」で検索し、対応できる
セキュリティ専門会社に依頼する

2）ルール化と定期的な見直し

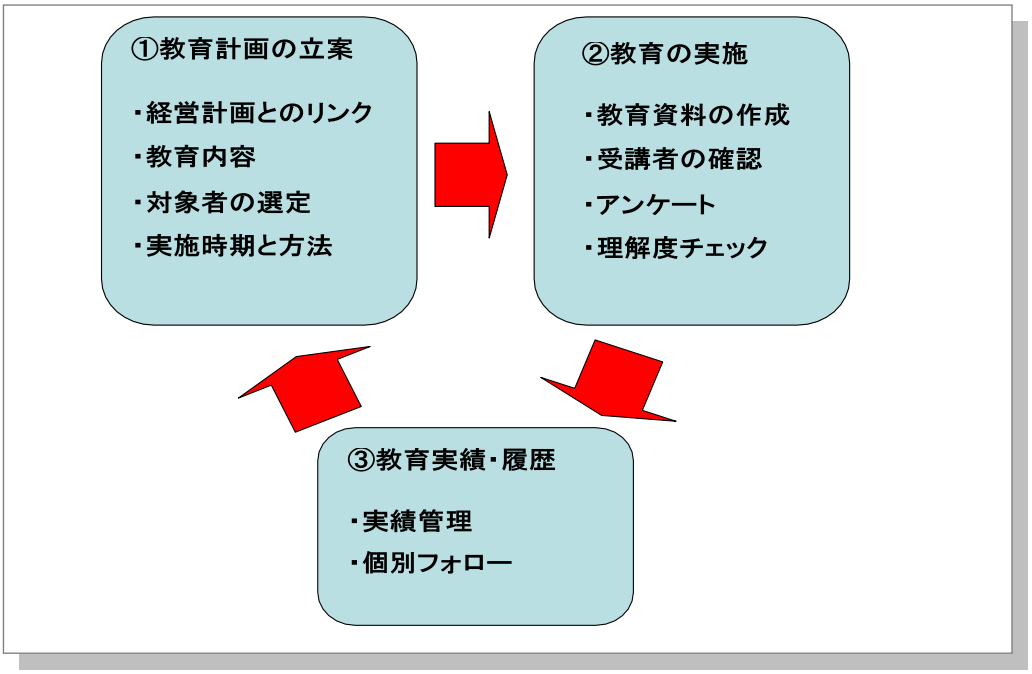
情報漏えいリスクを洗い出し、その情報漏えいリスクを回避する施策を決め、その施策を社内規定等に反映してルール化し、社員に周知すると同時に、定期的な見直しが重要となる。

（3）情報セキュリティ教育

協力会社に全員に情報セキュリティ教育を実施することが重要であることを説明してください。

推奨する主な教育内容

- 自社の情報セキュリティ方針の概要
- 作業所での情報セキュリティの必要性
- 請負業務ごとのルール、手順の確認
- 情報セキュリティ事故の対応方法と再発防止策
- 必須事項及び禁止事項の確認



【一般的な教育計画実施の流れ】

具体的な実施例

① 従業員への教育。二次以降協力会社等への指導・注意喚起。
② 定期的な教育以外に、新規採用時や中途入社時も実施する。
③ 新規の請負業務開始時や集合教育にて、請負業務に従事する関係者に対して、本ガイドラインや　参考資料−１「情報漏えい防止徹底について」を使用して、情報漏えい防止のための取り組みを周知教育する。
また、事故発生時に於ける顧客等の関係者への連絡対応も併せて周知する。
④ 作業所内で従事する作業員に対しては、送り出し教育時にて、添付資料−２「あなたが守るべき情報セキュリティ６か条」を使用して、最低限、実施すべき情報セキュリティ事項を教育する。守秘義務契約等がある場合には、追加で周知する。
⑤ 参考資料−２「各種ポスター」を活用して、情報セキュリティ意識の向上を図る。

（4）情報漏えいなどの事故発生時の対応

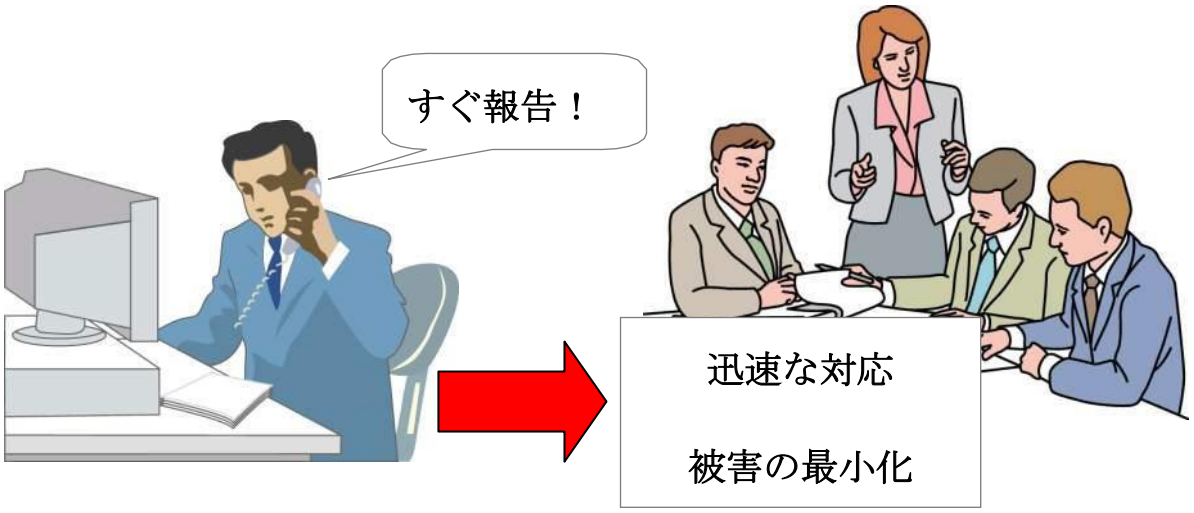
協力会社には、事前に情報漏えい等の事故が発生した時の対応の重要性と具体的な実施例について説明してください。

●事前に連絡体制を確立しておき、迅速に対応してください

情報漏えい および サイバー 攻撃の発生に備えて、事前に体制を確立しておき、すばやく行動・対処して被害を最小限に食い止める必要があります。

決めておくべき主なポイント

① どのように対応するべきか
② だれに連絡しなくてはならないか
③ 連絡ルートはどのようにするべきか



具体的な実施例

① 緊急時の対応手順、復旧・業務再開手順、緊急事故体制表を作成する。
② 情報漏えい および サイバー 攻撃において発生源となった場合は、 影響の及ぶ各社（元請会社および当該事故により影響がある取引先も含む） に対して、迅速に連絡する。
③ セキュリティ事故発生の原因と再発防止策を関係者全員に連絡し、周知徹底を図る。
④ 原因分析や再発防止策の策定には、ITベンダー等の外部の知見を活用する。

3.2　情報セキュリティにおける実施事例

以下、対策として特に重要な「情報セキュリティにおける実施事例」をあげます。協力会社にはこれを参考に情報漏えいのリスク軽減に努めるよう指導してください。

「情報セキュリティにおける実施事例」

（１）私有情報機器（パソコン、ＵＳＢメモリ、外付けハードディスク、スマートフォン等）の取扱いについて

（２）情報機器、書類等の盗難・紛失対策について

（３）ソフトウェア、クラウドサービス利用について

（４）ウイルス対策について

（５）電子メール対策について

（６）「情報」交換について

（７）「情報」保管について

（８）「情報」取扱いについて

（９）その他の情報セキュリティ対策について

（1）私有情報機器（パソコン、ＵＳＢメモリ、外付けハードディスク、スマートフォン等）の取扱いについて

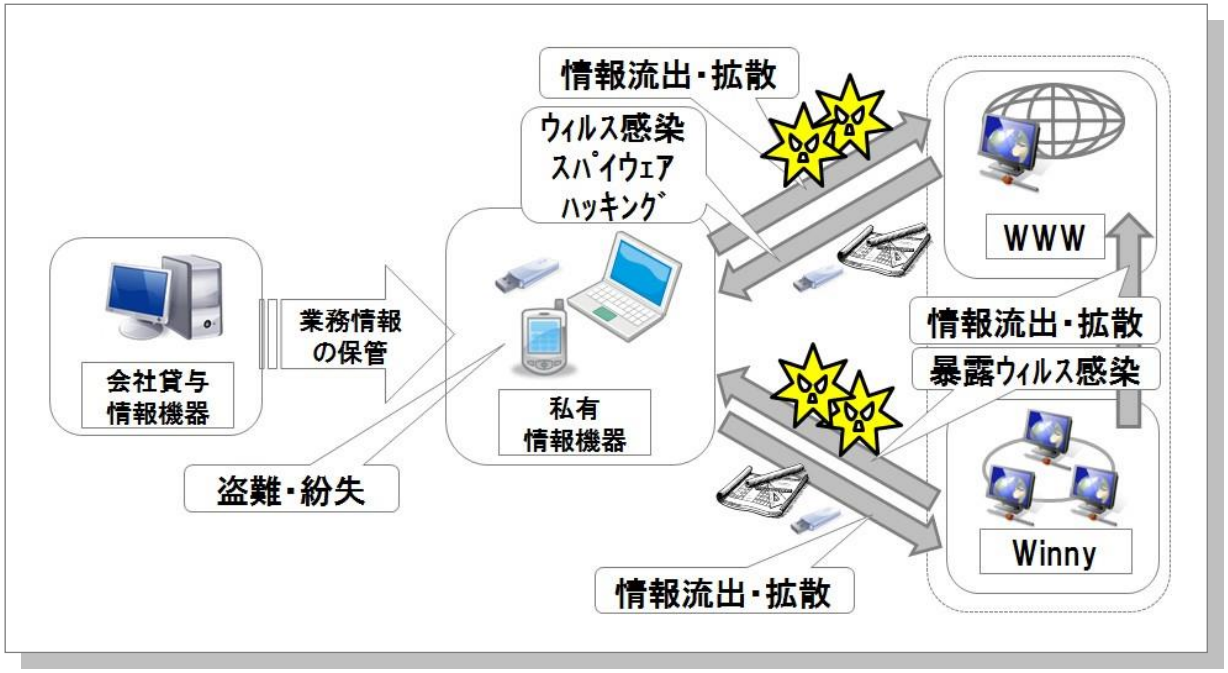
●私有情報機器利用は、情報漏えいする危険性を拡大させます

会社貸与情報機器について各種情報セキュリティ対策を一律に行っても、私有情報機器は、不十分となりがちです。以下の脅威により、情報がインターネット上に暴露・漏えいする恐れがあります。

① ファイル交換ソフトウェア（Winny 等）による情報漏えい
本人がファイル交換ソフトウェアを利用していなくても、家族が同一パソコンにてファイル交換ソフトウェアを利用していたため、ウイルス感染により情報が漏えいする事件が発生しています。

② ネットワークからのハッキングや暴露ウイルス感染
スマートフォンもパソコン同様の脅威が存在するため、情報セキュリティ対策が不十分であれば、情報が漏えいする恐れがあります。

※本件により、数多くの会社や官庁の業務データ等が漏えいし社会問題となっています。一度インターネット上に漏えいしたデータは拡散を続け、漏えいを止めることや回収することはできません。



【ウイルス侵入・情報流出経路】

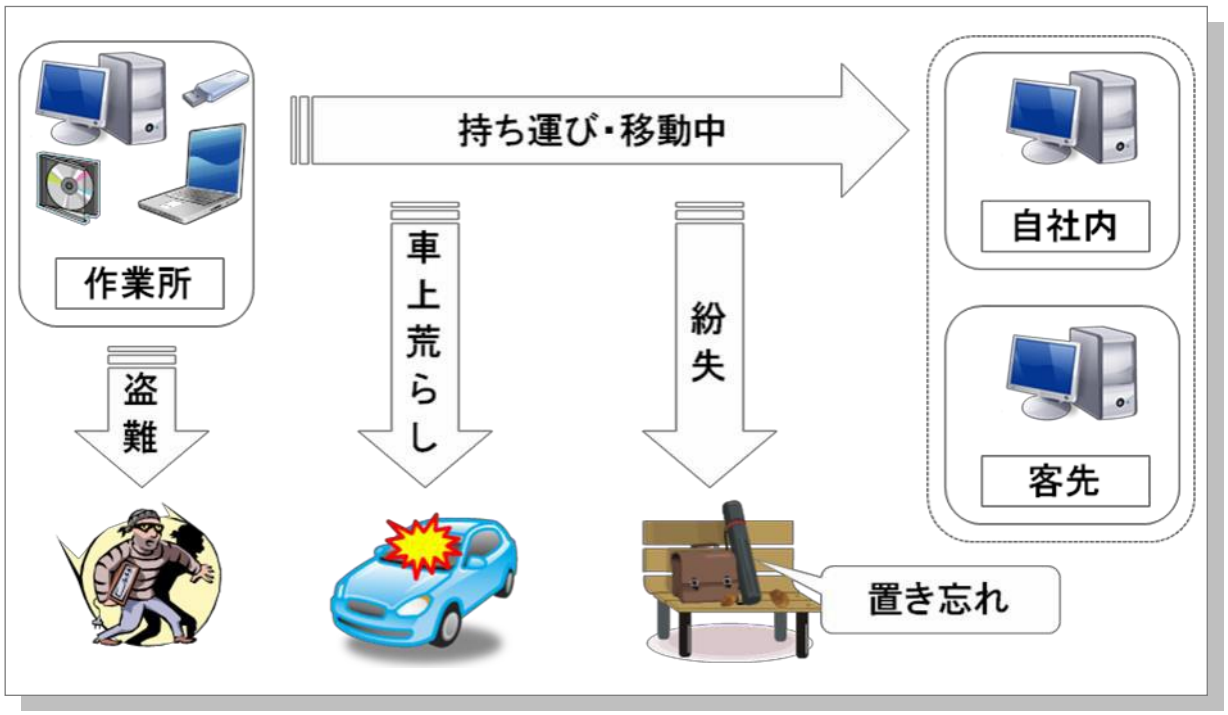
対策事例

① 私有情報機器に業務データを保管しない。
② セキュリティ対策を行った会社貸与情報機器を利用する。
③ 私有情報機器に業務データがある場合は直ちに削除する。
④ 会社貸与情報機器に私有情報機器を接続しない。

（２）情報機器、書類等の盗難・紛失対策について

●パソコン本体やハードディスク内の情報が狙われています

今や、情報が売れる時代です。泥棒もパソコン本体を売るためよりも、ハードディスク内の情報を売るためにパソコンを盗むとさえ言われています。当然、周辺機器・記憶媒体（ＵＳＢメモリ、外付けハードディスク、スマートフォン等）・書類も盗難の対象になります。まずは盗まれない対策、そして、万が一盗まれても 情報を抜き取らせない対策をとらなくてはなりません。紛失も同様で、紛失しない対策をとり、さらに紛失しても漏えいさせない対策をとらなければなりません。



【盗難・紛失による情報漏えい経路】

対策事例

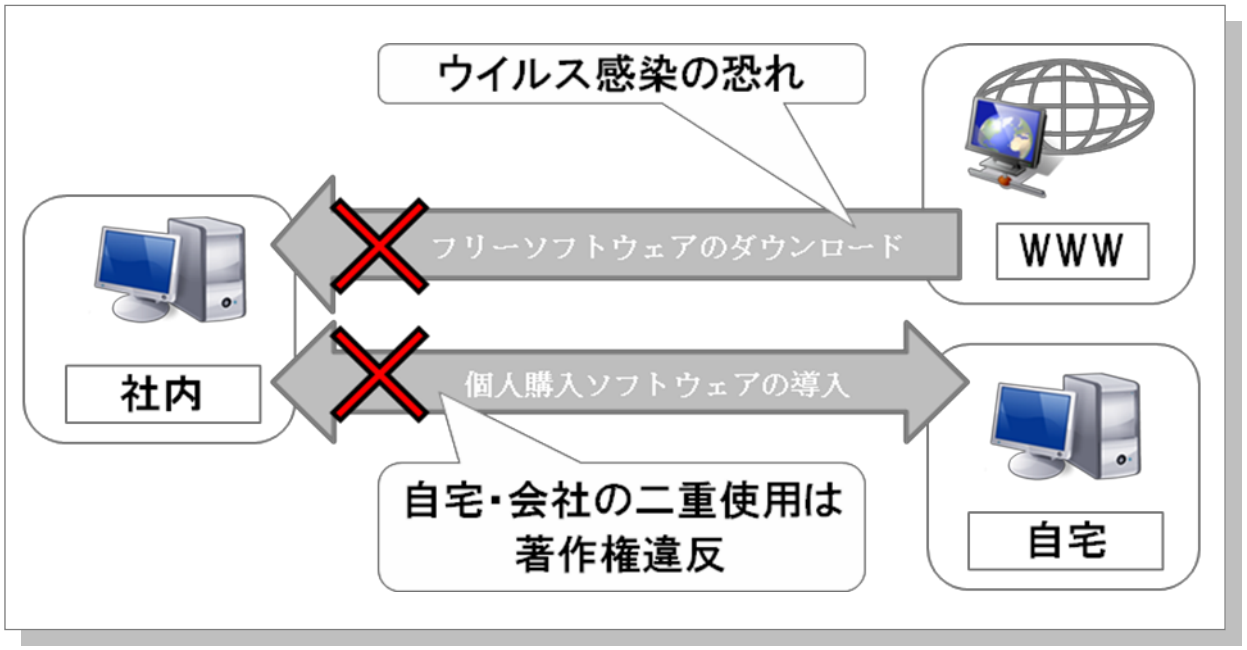
① 情報機器等を社外に持ち出す場合の社内ルールを決め、持ち出しを最小限にすると同時に持ち出し状況を管理する。
② 機械警備等、事務所の防犯対策を強化する。
③ パソコンにセキュリティロックワイヤをつける。また、持出しが容易なＵＳＢメモリや外付けハードディスク等は、施錠可能なキャビネット等に　保管する。
④ ログインパスワードの設定、パソコンのロック、ハードディスクの暗号化等の盗難・紛失に遭ってもデータを読み取らせない対策をとる。
⑤　図面、書類、記憶媒体を必要以上に持ち出さない。止むを得ず社外に持ち出す場合は、必要最小限とし、置き忘れ、盗難・紛失等の事故を防止する対策をとる。

（3）ソフトウェア、クラウドサービス利用について

●ウイルスの混入・ライセンス違反の恐れがあります

① 無料で使える便利なフリーソフトウェアも多い一方で、個人情報や機密データをハッカーに送り続けるウイルス(スパイウェア)をソフトウェアの中に潜ませているものがあります。安易にフリーソフトウェアを情報機器にインストールすることは大変危険です。また、無料で使えるクラウドサービスもセキュリティ対策が確実に行われず、保管された業務情報が漏えいする恐れのあるものもあります。クラウドサービスの選定にあたっては、日建連の“建設現場ネットワークの構築と運用ガイドライン”を参照する。

②適切なライセンスを取得していないソフトウェアを利用することは、法律に違反します。ソフトウェア開発会社からの損害賠償請求や、ライセンス管理のできない会社というイメージダウンにもつながります。ソフトウェアは、適切 なライセンスを取得したものを利用し、決して違法コピーをしてはいけません。



【ソフトウェア導入によるトラブル】

対策事例

① 個人の判断で勝手にソフトウェアをインストールしない。
② 正規に購入したソフトウェアのみを利用する。
③ 会社が許可するフリーソフトウェア、クラウドサービスを指定し、安全性や動作確認できないフリーソフトウェア、無料クラウドサービスは使用しない。
④ 情報漏えいの恐れのあるファイル交換ソフトは導入しない。
⑤ メーカーのサポート期限が終了したソフトウェアは使用しない。
⑥ クラウドサービスの利用においては、2要素認証や定期的なログ確認を実施

（4）ウイルス対策について

●ウイルス感染は、様々な被害を及ぼします

① ウイルスは、多種多様であり、感染すると次のような被害を及ぼします。

・情報機器を停止させる

・情報機器内の機密情報・個人情報・クレジットカード情報を盗み取る

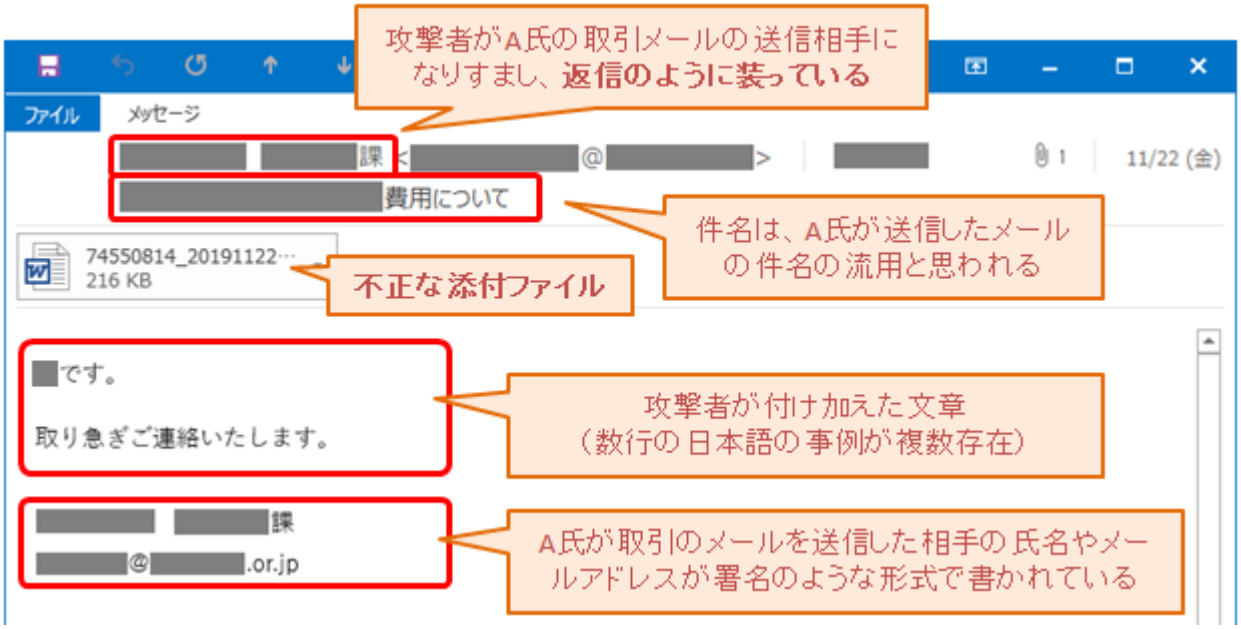
・他の人へ勝手にウイルス付きメールを送りつける

と様々です。ひどい場合は一台の感染から会社すべての情報機器が感染し、会社機能が停止することもあり得ます。

② ウイルスはそのプログラムを実行することで感染します。

・**身に覚えのない**メールを見る、添付ファイルを開かない

・怪しいホームページを見ない



【ウイルスメールの例】

出典：IPA Emotet（エモテット）と呼ばれるウイルスへの感染を狙うメールについて

対策事例

① パソコン、スマートフォンのＯＳ（Windows、Android 等）をＯＳのアップデート機能で更新し最新版にする。

② ウイルス対策ソフトウェアを導入し、最新の状態で常時起動する。

③ 知らない相手からの不審なメールは開かないで削除する。

フィッシング詐欺メール（AppleやMicrosoftを騙りIDとPWDを入力させ窃取を狙う）に注意。

④ 業務に関係ないホームページは見ない。

⑤ EDRを導入する。

（５）電子メール対策について

●業務で使うメールシステムは　Microsoft Officeやビジネス用Gmailなど、ウイルスや迷惑メールを駆除する機能を有する製品・サービスを採用することを基本とする。

① ウイルスや迷惑メール

・スパムメール

・広告宣伝メール

・架空請求メール

・フィッシング詐欺メール

・ウイルスメール

・怪しい副業メール

参照元：迷惑メールの6つの種類と正規との見分け方を解説

●誤送信は、情報漏えいと同じです

① 誤送信は悪意があろうとなかろうと、社会的には情報漏えいと言えます。送信前にもう一度送信先アドレスや添付ファイル等を間違えていないか確認します。

② 電子メールの宛先にも注意を払う必要があります。

- **「宛先」**　：メインの宛先（受信者には誰が受信したか分かります）
- 「ＣＣ」　：その他の宛先（受信者には誰が受信したか分かります）
- 「ＢＣＣ」　：見えない宛先（他の誰が受信したか隠すことができます）

メールアドレスも時には個人情報になるので、知られてよいのか否かを、考えて送らなければなりません。

※ 電子メールの受信者は、**他の人**にもメールが送信されたことが分かりますが、ＢＣＣ にアドレスが入力してある人については分かりません。

●重要情報は安易に送信しない

電子メールで添付ファイルを送る場合は、暗号化またはパスワードを掛けて送ります。また、パスワードは事前に取り決めておくか、別メールで送ります。

対策事例

① 送信前に必ず、送信先アドレスの確認を行う。
② 重要情報を電子メールで送信する場合は、
暗号化またはパスワードを掛けて必ず保護する。
③ お互いのメールアドレスを知らない複数人にメールを送信する場合は、「ＢＣＣ」を利用する。

（６）「情報」交換について

●関係者に渡す情報は最小限にとどめます

社内・社外を問わず、コピー、ＦＡＸ、郵便物、電子メールを使用する場合は、内容、相手先、部数を再確認して、必要最小限にとどめる注意が必要です。

●社外とのデータ交換

社外とデータの受け渡しをする場合は、第三者によるアクセスや盗難等の脅威から保護するための対策及びルールが必要です。

対策事例

① 渡す情報は最小限にとどめる。
② 情報を相手に渡す場合は、内容・相手先・部数をよく確認する。
③ 重要文書の場合は必ず、管理台帳を作成し、回収・返却を確認するまで管理する。
④ ＵＳＢメモリ等の外部記憶媒体でデータの受け渡しをする場合は、暗号化等のセキュリティ機能付きの機器を使用する。

●ファイル交換サービス・クラウドストレージの利用

利用シーン
- 社内/社外とのデータのやり取り
- 機密情報を含んだデータのやり取り
- 大容量のデータのやり取り

特長
- リンク記載方式
- データ受け渡し期間を設けることが可能

メリット
- システム内でウイルス対策されている
- 誤送信の場合、URLリンクを無効にすることで情報漏えいを防ぐことが可能

（７）「情報」保管について

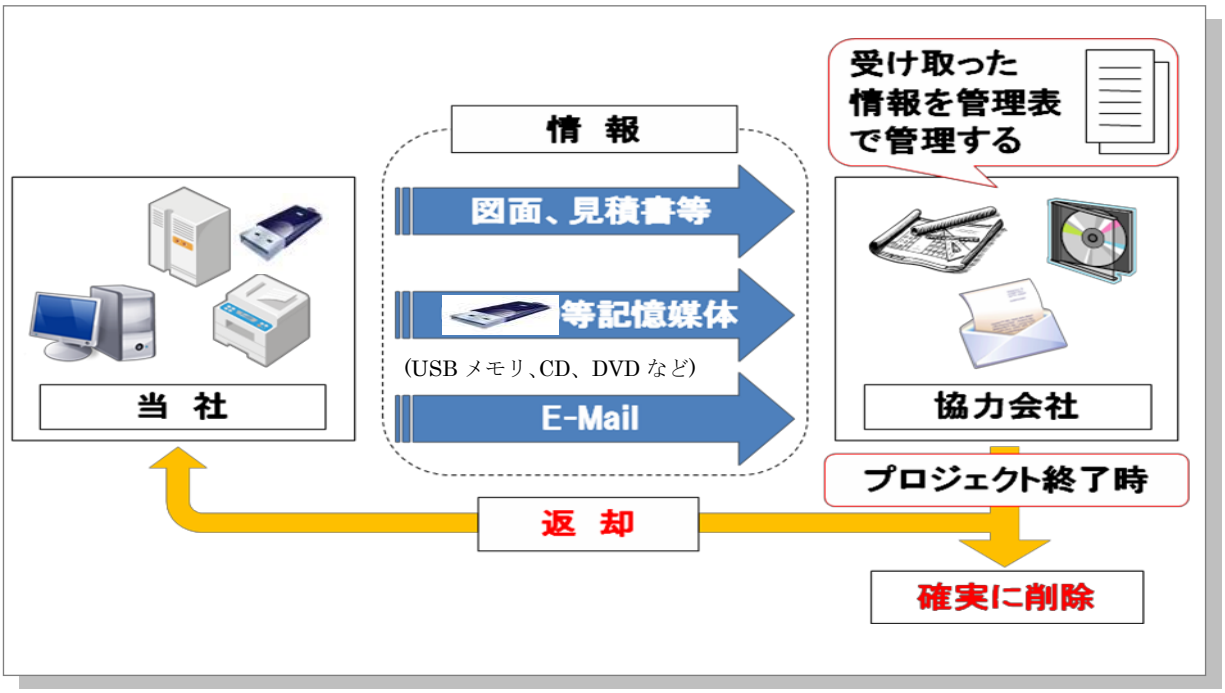
●最善の情報漏えい対策は、情報を持たないことです

情報漏えいを防ぐための一般的な対策として暗号化やパスワード設定がありますが、最善の対策は、情報漏えいして問題になるような情報を持たないことです。情報機器や記録媒体に保存され利用が終了した情報は、消去ソフトウェアを利用するなど、情報を確実に消去する措置が必要です。

●情報を持った場合は、それを利用できる人を最小限にすることです

一般的には

- 情報漏えいを防ぐためのウイルス対策で保護された安全なサーバーに保存する。
- 情報を閲覧、編集できる社員へのアクセス権は、最小限にとどめる。
- 当該情報へのアクセスログは1年以上保管する。



【利用が終了するまでの情報の運用方法】

対策事例

① 情報および情報機器の授受に関する会社のルールを遵守する。

② 元請会社・取引先・発注者から預かった情報は、管理表等に記載し厳重に管理する。

③ 業務が終了した時点で、元請会社・取引先・発注者から預かった情報や必要のない情報は廃棄する。

・書類（紙情報）は読めないようにして処分する。（溶解又はシュレッダー等）

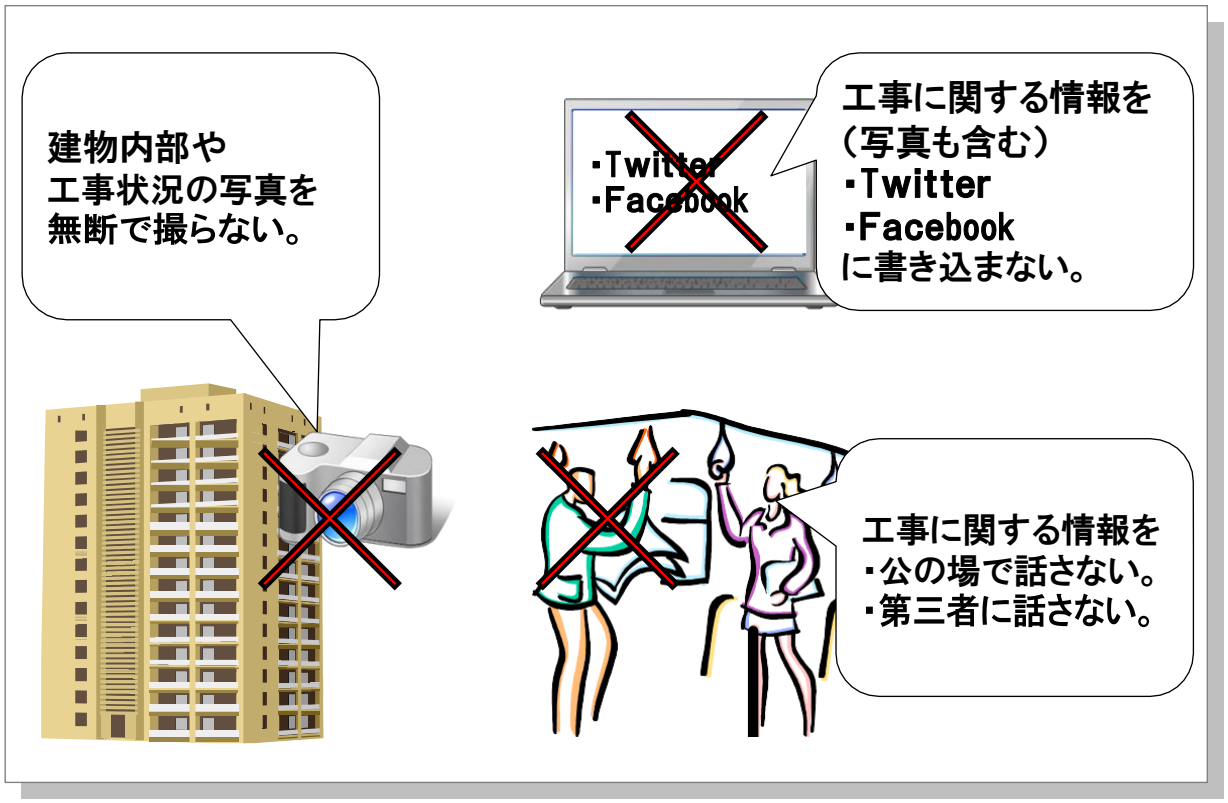
・パソコンや記憶媒体を廃棄する場合は、電子データを読めなくして処分する。

（物理的な破壊又は完全抹消ソフトによる消去等）

（８）「情報」取扱いについて

●工事に関する情報は、発注者のものです

工事に関する情報の所有権は、発注者にあります。よって、無断で情報を持ち出したり、利用したりすることは契約違反などの問題になります。



【禁止事項】

対策事例

① 工事に関する情報を第三者に口外しない。
② 工事に関する情報を、Facebook やTwitter 等に書き込まない。
③ 工事に関係する情報を無断で持ち出さない。
④ 建物内部や工事状況の写真を無断で撮らない。
⑤ 工事に関する情報を目的以外で利用しない。

（9）その他の情報セキュリティ対策について

●個人情報保護

個人情報保護法に基づいて個人情報の適正な取扱いを確保するための対策を行ってください。

●ネットワーク

社内は、第三者がアクセスできないように適切に管理してください。

作業所では、日本建設業連合会発行の参考資料－３「建設現場ネットワークの構築と運用ガイドライン」に準拠して実施してください。

●バックアップ

重要情報は情報機器の故障や誤操作、紛失等によって消失しないように、バックアップ等の対策を行ってください。

具体的には、

- データバックアップの実施と復旧方法を策定する。
- バックアップデータは、災害時の事業継続に備え、遠隔地にも保管することが望ましい。

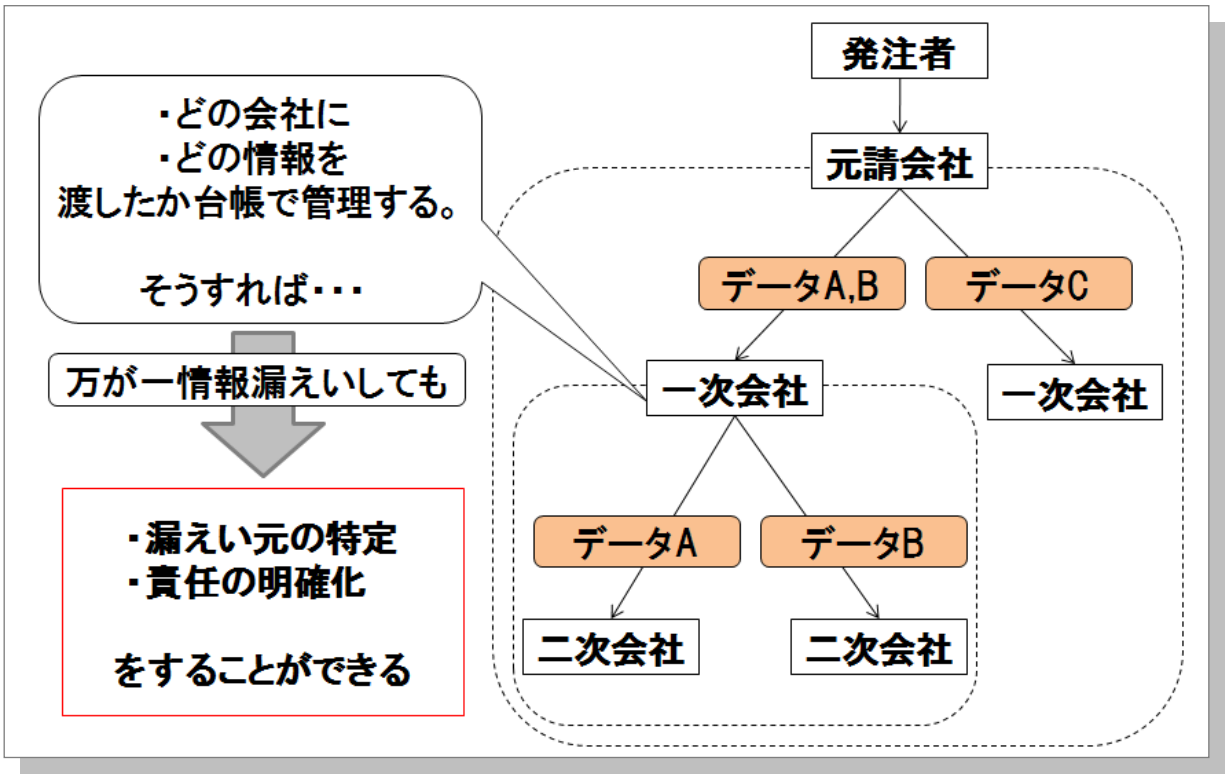
3.3　二次以降協力会社への留意事項について

一次協力会社に対して、二次以降の協力会社の情報セキュリティについても重要であり必要とされる対応について説明してください。

●二次以降協力会社での情報セキュリティ事故も多く発生しています

情報セキュリティ事故は、二次以降協力会社で発生することも少なくありません。万が一、二次以降協力会社において情報漏えいが発生した場合、実際に情報漏えいを起こしたのは二次以降協力会社であっても、自社や元請会社を含め、事故の責任を問われることがあります。情報を二次以降の協力会社へ渡す場合には細心の注意を払う必要があります。

なお、一次協力会社が二次協力会社に情報セキュリティ強化を図る際には、二次協力会社への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の構築に向けて（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」に留意するように指導してください。



【二次以降協力会社での情報管理】

（１）二次以降協力会社の元請会社への報告

一次協力会社が、二次以降協力会社を置く場合は、適正な施工体制の確保に加え情報セキュリティの観点からも、必ず元請会社の承認を得る必要があります。

（２）元請会社から求められた情報セキュリティ対策について

一次協力会社には、元請会社から求められている情報セキュリティに関する要請について、二次以降の協力会社にも必要に応じた対応をお願いする。

＜主な内容事例＞

・守秘義務
・体制（情報セキュリティ管理者・担当者の決定）
・情報の管理（紙、電子データの取扱い、メール）
・パソコンなど情報機器の管理（ウイルス対策、ソフトの不正利用をしない、私有情報機器に業務情報を保管させない
・情報セキュリティ事故発生時の対応

（３）二次以降協力会社と機密保持に関する契約を締結

一次協力会社が、二次以降の協力会社と契約書や業務委託を交わす際には、下記の情報の取扱いに関する事項も含めるよう指導する。

＜情報の取扱いに関する項目例＞

- 機密保持
- 対象範囲
- 情報の管理
- 事故発生時の対応
- 契約期間終了時の対応（情報の返却、廃棄）
- 契約期間終了後の機密保持を継続させる期間

（４）二次以降協力会社に渡した情報の管理

一次協力会社には、元請会社から要請があった工事の情報については、二次以降協力会社に提供した情報を管理台帳で管理していただくとともに、契約終了時には、提供した情報の回収・廃棄する。

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「情報セキュリティチェックシート（経営層・情報セキュリティ責任者用）」

添付資料－２「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）」

参考資料について

日本建設業連合会のホームページからダウンロードし、利用してください。

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

参考資料－１「情報漏えい防止について」

参考資料－２「各種ポスター」

参考資料－３「建設現場ネットワークの構築と運用ガイドライン」

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「協力会社における情報セキュリティガイドライン」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

2023年2月の改定について

サイバー攻撃やランサムウェア攻撃の被害増加に対応して、追加施策を追加

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の構築に向けて（令和4年10月28日　経済産業省、公正取引委員会）」の遵守事項について修正

執筆委員：最新版（敬称略、五十音順）

市橋　章宏（清水建設）	葛原　徹（大成建設）	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）	滝沢　強（前田建設工業）
田口　慶（鹿島建設）	藤井　隆行（東急建設）	豆腐谷　洋一（竹中工務店）
藤田　直紀（戸田建設）	山口　正志（フジタ）	

執筆委員：初版

相澤　健次郎（大林組）	石垣　順史（清水建設）	大塚　暁　（鹿島建設）
小倉　弘至（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）	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）

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