



情報セキュリティ専門部会 報告

✓「建設現場ネットワークの構築と運用ガイドライン」
(平成25年9月発行) について

✓その他一専門部会の取組み

2014/2/13「建築のITセミナー」資料

○ガイドラインについて

建設現場ネットワークの 構築と運用ガイドライン

平成25年9月

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	1
1.1	ガイドラインの範囲	1
1.2	展開と取扱いについて	1
2.	ネットワーク構成	2
2.1	共通事項	3
2.2	現場事務所内ネットワーク	4
2.3	企業内ネットワーク及びインターネットへの接続	5
2.4	施工現場でのネットワーク	8
2.5	外部関係者との情報共有	10
3.	ネットワーク維持管理	12
3.1	ネットワーク担当者の選定	12
3.2	ネットワーク担当者の役割	12
3.3	JV 現場における考慮事項	13
4.	ネットワークのセキュリティ	14
4.1	LAN 共有時の対策	14
4.2	回線共有利用時の対策	14
4.3	無線 LAN 利用時の対策	16
4.4	共有サーバー（NAS）利用時の対策	17
4.5	クラウド利用時の対策	18
4.6	スマートデバイス利用時の対策	19
4.7	バックアップ・リカバリー対策	20
4.8	WEB カメラ利用時の対策	21
5.	JV 現場ネットワーク構築手順と事例	22
5.1	手順	22
5.2	事例	23

○付録

○あとがき



○ ガイドラインの解説

【1. はじめに】

✓ガイドライン作成の経緯

(これまで作成したガイドライン)

- ・「JV現場ネットワークの構築と運用ガイドライン(2005/4)」
JV現場事務所内での情報共有における
「効率化」と「安全確保(情報セキュリティ対策)」
- ・「建設現場における情報セキュリティガイドライン(2008/11)」
建設現場事務所に焦点を絞ったセキュリティ対策



○ガイドラインの解説



【1. はじめに】

✓ガイドライン作成の経緯

(新たな課題)

- ・ICTの進化＋建設現場での利用増加

無線技術、スマートデバイス、クラウド、事務所-現場間の情報伝達

- ・セキュリティ脅威の増加

サイバー攻撃、新技術の脆弱性、なりすまし、踏み台、????



ガイドライン作成(見直し)が必要

Point !



「セキュリティリスクの注意点を明確にし、新技術や実運用に対応」

○ガイドラインの解説



【1. はじめに】

✓ガイドラインの目的と位置づけ

○建設現場ネットワークの安全・安定した運用

○建設現場への容易な導入

・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)」を「現在の技術レベル」「運用レベル」に照らして見直し

・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(第1版)」との棲み分けを図り、全面的に再編集

・再編集に際しては、JV現場だけに限らずに単独現場も含めて対象

・ICT(情報通信技術)の進歩に伴い増大しているクラウドサービスやスマートデバイス・無線LAN等の利用に際してのセキュリティリスクへの対応策を追加

○ガイドラインの解説

【2. ネットワーク構成】

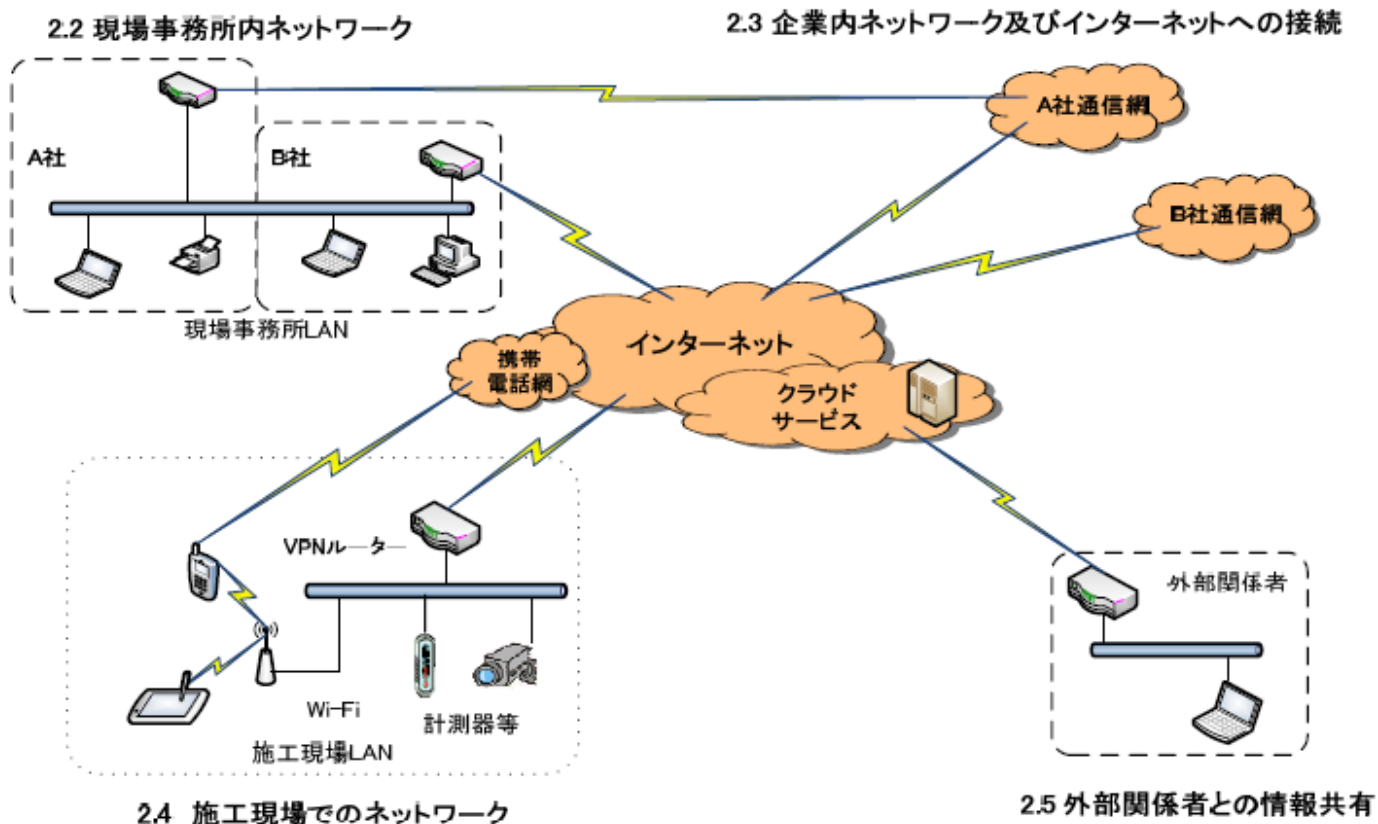


図 2-1 建設現場ネットワーク例



○ガイドラインの解説



【2. ネットワーク構成】

✓2.1 共通事項

- 1) LAN方式 2) 通信プロトコル 3) ネットワークセグメント
- 4) アクセス回線 5) インターネットへの接続
- 6) モバイル通信サービスの利用 7) JV構成会社への接続
- 8) 協力会社、設計事務所等の接続 9) スマートデバイス
- 10) 外部関係者との情報共有

Point !



「無線LAN、複数セグメント、スマートデバイス、クラウド」

○ ガイドラインの解説

【2. ネットワーク構成】

✓ 2.2 現場事務所内ネットワーク

- 1) IPアドレス
- 2) 共有サーバー
- 3) プリンター・複合機
- 4) ネットワーク構築における留意事項

Point !



「運用効率化の具体策、セキュリティ観点での具体策」



○ ガイドラインの解説



【2. ネットワーク構成】

✓2.3 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
- 2) インターネットへの接続
- 3) モバイル通信サービスでの企業内ネットワーク接続
- 4) JV現場における回線の共有

Point !



「接続方法の例示、セキュリティリスクの解説」

○ ガイドラインの解説

【2. ネットワーク構成】

✓ 2.4 施工現場でのネットワーク

- 1) 施工現場と現場事務所とのネットワーク接続
- 2) 施工現場や現場事務所でのスマートデバイスの接続

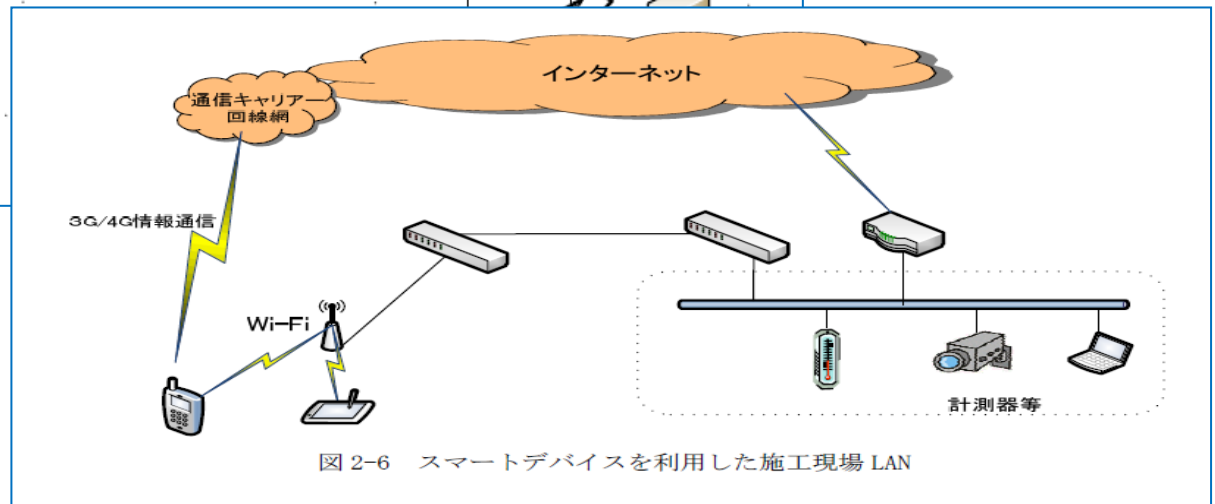
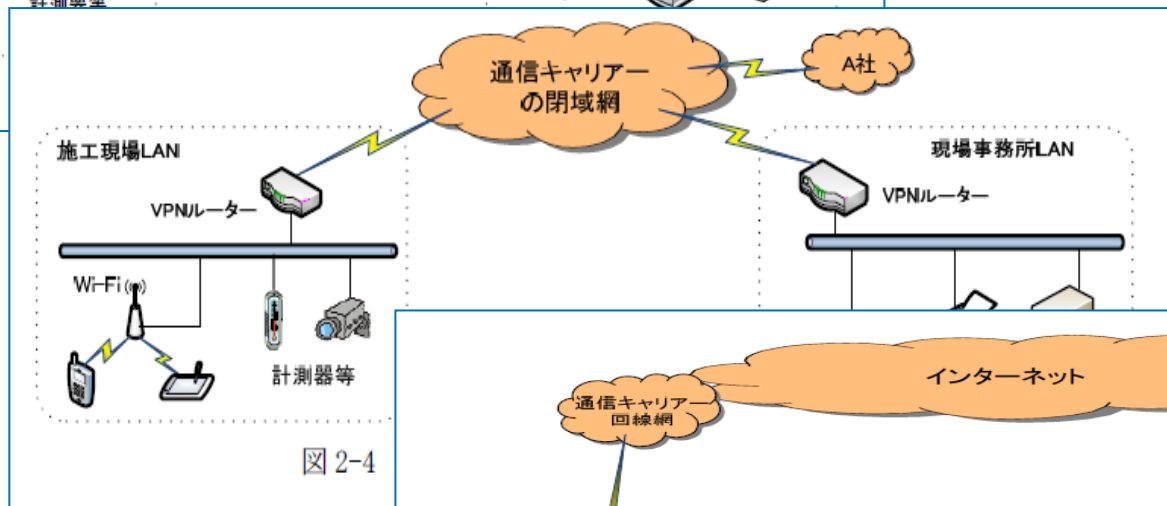


Point !



「施工現場に焦点、パターン別図による解説」

○ガイドラインの解説



○ ガイドラインの解説



【2. ネットワーク構成】

✓2.5 外部関係者との情報共有

- 1) クラウドサービスの利用イメージ
- 2) クラウドサービス利用上の注意点
- 3) Webカメラの取り扱い

Point !



「外部との情報共有はクラウドが基本、Webカメラの注意点」

○ガイドラインの解説



【3. ネットワーク維持管理】

- ✓3.1 ネットワーク担当者の選任
- ✓3.2 ネットワーク担当者の役割
- ✓3.3 JV現場における考慮事項

- ・「機器」「ネットワーク回線」「ソフトウェア」「IPアドレス」「周辺機器」の管理
- ・セキュリティ管理
- ・費用負担
- ・障害時対応

Point !



「管理手法の例示、管理資料の雛形」

○ ガイドラインの解説

【4. ネットワークのセキュリティ】

✓4.1 LAN共有時の対策

- 1) ネットワークの構成
- 2) 情報共有サーバーの配置
- 3) 複合機等の共有機器の配置
- 4) 対策例

Point !



「ネットワーク管理者の行う対策例を例示」



○ ガイドラインの解説

【4. ネットワークのセキュリティ】

✓4.2 回線共有利用時の対策

- 1) 複数の接続が設定可能
- 2) 回線共有の構成
- 3) セキュリティ上の対策例



Point !



「JV構成会社毎のアクセスが基本、共有時の対策を説明」

○ ガイドラインの解説

【4. ネットワークのセキュリティ】

✓ 4.3 無線LAN利用時の対策

- 1) ネットワーク関係者の承諾
- 2) APのセキュリティ設定
- 3) 無線LAN設定情報の管理者の選任
- 4) 無線LAN子機の管理
- 5) 電波干渉、カバレッジホールの回避
- 6) APへの電源供給

Point !



「運用を適切に行わないと情報漏えいのリスクが高い」



○ ガイドラインの解説

【4. ネットワークのセキュリティ】

✓ 4.4 共有サーバー(NAS)利用時の対策

- 1) ユーザーの管理
- 2) フォルダーのアクセス権
- 3) ウィルス対策
- 4) サーバーデータの保護
- 5) 盗難防止対策

Point !



「基本的な事項を再徹底する」



○ ガイドラインの解説

【4. ネットワークのセキュリティ】

✓ 4.5 クラウド利用時の対策

- 1) クラウドサービス利用に関する対応
- 2) クラウド接続に関する対応
- 3) 発注者からの要請により利用する場合の注意点

Point !



「事前(契約)、運用(PC対策)、終了時の取扱」



○ ガイドラインの解説

【4. ネットワークのセキュリティ】

✓ 4.6 スマートデバイス利用時の対策

- 1) 携帯電話としての管理
- 2) 企業間でセキュリティポリシーが異なる場合
- 3) スマートデバイスに関するセキュリティ対策の具体例

Point !



「ルール作成、誓約、強制(MDM)、限定(データ非保存)」



○ ガイドラインの解説

【4. ネットワークのセキュリティ】

✓ 4.7 バックアップ・リカバリー対策

- 1) 現場事務所内でのバックアップ
- 2) 現場事務所外へのバックアップ

Point !



「故障、ウィルス感染、盗難、自然災害」



○ ガイドラインの解説

【4. ネットワークのセキュリティ】

✓ 4.8 WEBカメラ利用時の対策

- 1) インフラについて
- 2) WEBカメラについて
- 3) その他

Point !



「機器環境のちがい毎に対策を例示」



○ ガイドラインの解説



【5. JV現場ネットワーク構築手順と事例】

✓5.1 手順

✓5.2 事例

- ・「JV運営委員会での運営方法の提示」～「運用」までの手順
- ・「各種管理表」及び「JV現場ネットワーク構成図」の例示

Point !



「運用開始までの具体的な手順」

○ ガイドラインの解説



【付録】

付録-1 (JV 現場ネットワーク管理資料ひな型)

様式-1 ネットワークアドレス一覧表

様式-2 各社ネットワーク担当者一覧表

様式-3 情報処理関連設備の費用分担表

付録-2 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)

付録-3 JV現場における無線LAN 利用申請書(例)

付録-4 (参考)

参考資料-1 用語解説(本書での用語定義)

参考資料-2 よくあるトラブルの要因

参考資料-3 電波法・電気通信事業法の説明

○ガイドラインの解説

【付録】



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)

付録-2

株式会社幹事会社A (以下「甲」という。)、株式会社構成会社B (以下「乙」という。)、構成会社C 株式会社 (以下「丙」という。)) (以下甲・乙・丙を総称して「構成員」という。))とは、〇〇〇〇年〇月〇〇日付にて構成員間で締結した共同企業体協定書に付帯して、共同企業体内での電子情報の取り扱い及びネットワークシステムに関し、以下の事項について合意した。

第1条 目的

本覚書締結は共同企業体内での電子情報の取扱い及びネットワークシステムに関わる不正行為を防ぐことを目的とする。

電子情報の取扱い及びネットワークシステムに関わる行為を以下に示す。

- ①共同企業体内での電子的な情報交換。
- ②構成員の自社の企業内ネットワークへの接続。
- ③発注者、設計者、コンサルタント、協力会社及び自社本店等とネットワークを介しての電子的な情報交換。

第2条 責任と役割

- 1 構成員は、共同企業体内で情報共有を行なうに当たり、本覚書締結事項を遵守し、信義を重んじ誠実に運用にあたらなければならない。
- 2 構成員は、業務の遂行上知り得た共同企業体及び自社以外の業務上の秘密情報及び技術情報などを第三者に開示、漏洩又は提供してはならない。
- 3 構成員は、本条を遵守させるために必要な措置を講ずるものとする。
- 4 本条の規定は、共同企業体解散後も効力を有するものとする。

第3条 禁止事項

構成員は、以下に定める事項の遵守を徹底しなければならない。

- ①共同企業体内の他の構成員固有データの盗用・破壊・改ざんの禁止。
- ②共同企業体内固有データの業務外使用の禁止。
- ③他の構成員が保有する独自システムへの侵入禁止。
- ④上記に定める事項のほか、別途運営委員会が制定した禁止事項。

第4条 違反時の処分規定

構成員が本覚書において定めた事項に違反した時は、当該構成員は運営委員会の決定した処分に従わなければならない。

第5条 その他の取決め

構成員は、本覚書並びにガイドラインに定めのない事項又は疑義のある事項が生じたときは運営委員会において定めるものとする。本覚書の全部又は一部を変更する場合も同様とする。上記締結の証として、本覚書3通を作成し甲・乙・丙記名押印の上、各々1通を所有するものとする。

〇〇〇〇年〇月〇〇日

甲

乙

丙

JV現場における無線LAN利用申請書(例)

付録-3

平成 xx 年 xx 月 x 日

〇〇〇〇〇〇JV 工事事務所
所長殿

株式会社 〇〇〇〇〇〇

〇〇〇〇職員にタブレット端末を利用させる件 (依頼)

当社は生産性向上、業務の効率化を目的に当社現場職員に対し、タブレット端末の利用を展開しております。タブレット端末の利用にあたってはネットワークへの接続が必要となりますが、同機は無線LAN接続にしか対応していません。

一般社団法人 日本建設業連合会 (日建連) では「建設現場ネットワークの構築と運用ガイドライン」にて無線LANの利用にあたり、「一部でも無線LANを導入する場合には、JV 現場ネットワーク全体のセキュリティに影響を与えるため、導入前にはJV 構成会社全体の承認を得る。」と規定されており、今回本ガイドラインに則り、無線LANでの接続を許可頂きたいをお願いするものです。

なお、今回設置を希望する無線LAN機器は、配布するタブレット端末に「電子証明書」を搭載したもののからのアクセスしか受け付けない仕様で、現段階で無線LANの接続では最も安全な方式となっております。

つきましては、下記の通り無線LAN環境を構築したくご検討願います。

記

1 設置する無線LAN機器

〇〇〇〇製 〇〇〇〇

2 無線LAN接続時の認証方式

WPA2 エンタープライズによる認証

※「WPA2 エンタープライズ」とは

通常、無線LANに接続する場合にはSSIDと呼ばれるIDとパスワードが揃えば第三者が不正にアクセスできる可能性があります。WPA2 エンタープライズは当社内に設置されたサーバーが発行する「電子証明書」をタブレット端末にインストールし、この電子証明書で認証を行います。したがってID、パスワードによる認証は行なっていません。また電子証明書はコピー又は偽造することができないため、現段階で無線LANの接続では最もセキュアな認証方式です。

3 タブレット端末のセキュリティ対策

万一の盗難、紛失に際しては、取得者がタブレット端末を利用できないようパスワードによるロックを必須とし、規定回数以上の入力ミスがあった場合は、タブレット端末上のデータを全て削除する対策を講じています。また、暗号化機能を有効にし、MDM (モバイルデバイス管理) の採用により、ネットワーク接続下でリモートワイプ、リモートロック機能によりデータを保護・削除します。

4 本件に関する問い合わせ先及び資料提出先

株式会社〇〇〇〇

Tel :

Mail :

以上

○その他(セキュリティツールの紹介)

パンフレット「情報漏えい防止徹底のお願い」 1/2



協力会社作業員向け
情報セキュリティ教育資料

協力会社のみなさんへ

～情報漏えい防止徹底のお願い～

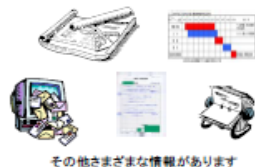
情報管理も大事な仕事のひとつです

配布元会社名

近年、情報漏えいに関する事故がテレビ・新聞等で大きく報道されています。一旦、このような事故が起こると会社だけでなく、個人に対しても厳しく責任が追及されます。このような事故を未然に防ぐために、この資料に書かれているポイントをよく理解して、情報漏えい防止に努めてください。

工事に関する「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）
- みなさんの会社の管理情報



その他さまざまな情報があります

もし、あなたの過失で「情報」が漏れてしまったら・・・>>>
万が一「情報」が漏れいしたら、どのような事態を招くことになるのでしょうか？

- 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。
- 法律や契約等に抵触し、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、守秘義務契約など



なぜ、どうして「情報」が漏れたの・・・>>>

ほとんどが不注意や認識不足。まさか漏れるとは思っていませんでした。

- 私物(自宅)パソコンで仕事をしていて、ちゃんと設定すればWinny(ウニー)も大丈夫と思っていたが、ウイルスに感染してパソコンに保存された業務データや電子メールがすべて流出した。
- パソコンを電車で置き忘れたら、ネットオークションで販売されてデータも流出した。
- 工事情報や個人情報を保管した USB メモリを紛失した。



「情報」を守るための9つのポイント

万一情報漏えい事故を起こしてお互いに迷惑をかける前に、ここに書かれた最低限の守るべきポイントを日頃から守ってお互いの信頼関係を築いてゆきましょう。

ポイント1 工事に関する「情報」は絶対に口外しない >>>

- お客様、近隣住民、工事関係者の個人情報の取扱いに注意してください。
 - 個人情報の管理は、法律でも厳しく定められています。過失による個人情報の流出でも、会社だけでなく個人も罰せられる可能性があります。
- 工事に関する情報は、絶対に口外しないでください。
- 次のような行為はもちろん禁止です。
 - 工事に関する情報を、インターネットのブログ(個人日記)や掲示板(2ちゃんねるなど)に書き込む。
 - 工事関係者や工事関連会社のリストを無断で持ち出す。
 - 建物内部や工事状況の写真を無断で撮る。



ポイント2 しっかりと保管しましょう >>>

- 図面、書類や外部記憶媒体(USBメモリ、CD、DVDなど)は、決められた場所に保管してください。
- 特に重要な情報が記録されたものは、鍵を掛けて保管してください。
 - 事務所荒らしによるパソコンの盗難が多発しています。事務所に防犯対策を施すことも大切です。



○その他(セキュリティツールの紹介)

パンフレット「情報漏えい防止徹底のお願い」 2/2



ポイント3 Winnyなどのファイル交換ソフトを入れない >>>

- 業務で使用するパソコンにファイル交換ソフトを絶対インストールしないでください。
- 代表的なファイル交換ソフトは、以下の通りです。
Winny(ウニー), Share(シェア), Cabos(カボス), LimeWire(ライムワイヤ)など



ポイント4 私物パソコンを業務に使わない >>>

- 私物のパソコンを業務に使用しないでください。
- 私物パソコンは、ウイルスやスパイウェアなどで情報流出のリスクが高いです。
- 私物パソコンに業務データがある場合は直ちに削除してください。
- 業務に使用するパソコンを私的に利用したり、家族と共用したりしないでください。

例: 家族が共用パソコンに Winny を導入し、ウイルスに感染したため情報が漏えいした。



ポイント5 ウイルス対策ソフトは必ずパソコンに入れましょう >>>

- パソコンには、ウイルスを検知・駆除するためのウイルス対策ソフトを必ず入れてください。
(パソコンショップで、数千円程度で市販されています)
- ウイルス対策ソフトは、常に最新の状態に更新してください。
- マイクロソフトのセキュリティ修正プログラムは適宜適用してください。



ポイント6 パソコンには、必ずパスワードを設定しましょう >>>

- 使用するパソコンには、必ずログインパスワードを設定してください。
- パソコンや業務システムを利用する際に使う金庫の鍵のようなものです。万一の盗難や不正利用のリスクを最小限にしてくれます。
- パスワードは、他人に推測されにくいものにしてください。
- パスワードは他人に漏れないように管理してください。
(紙に書いて貼っておくことは厳禁です)



ポイント7 「情報」の持ち出しや持ち歩きには注意しましょう >>>

- 図面、書類やパソコン、外部記憶媒体を必要以上に職場から持ち出さないでください。
- パソコン、外部記憶媒体を持ち出す場合には、暗号化やパスワード設定など盗難・紛失時のリスク回避策を行ってください。
- 職場の外では肌身離さないよう注意してください。電車の網棚に置いたり、車中に放置したりしてはいけません。
- 持ち出し時には、目的地に直行してください。



プライベートな要件などの寄り道は気の緩みが生じ、事故のもととなります。

ポイント8 コピー、FAX、郵送、メールの使用は最小限にとどめ、誤配に注意しましょう >>>

- 関係者に渡す「情報」は最小限にとどめてください。
- 郵送、FAX、電子メールなどで「情報」を送信する際には、宛先や送付する書類に間違いがないかよく確認してください。
- 重要な情報を電子メールで送信するのは控えてください。やむを得ず送信する場合は、必ず暗号化をおこなうか、パスワードを設定してください。



ポイント9 「情報」は確実に返却・廃棄しましょう >>>

- 工事が完了したら、保管の必要な情報以外は全て返却または廃棄してください。廃棄する際は図面、書類やパソコンから情報が盗みだされることが無いよう、次の対策を実施しましょう。
- 図面、書類はシュレッダーにかける。
- CD、DVD 等の外部記憶媒体はハサミで裁断するなど、物理的に破壊する。
- パソコン内の不要なデータを削除する。(ごみ箱からも必ず削除する)



もしも「情報」が漏えいしてしまったら

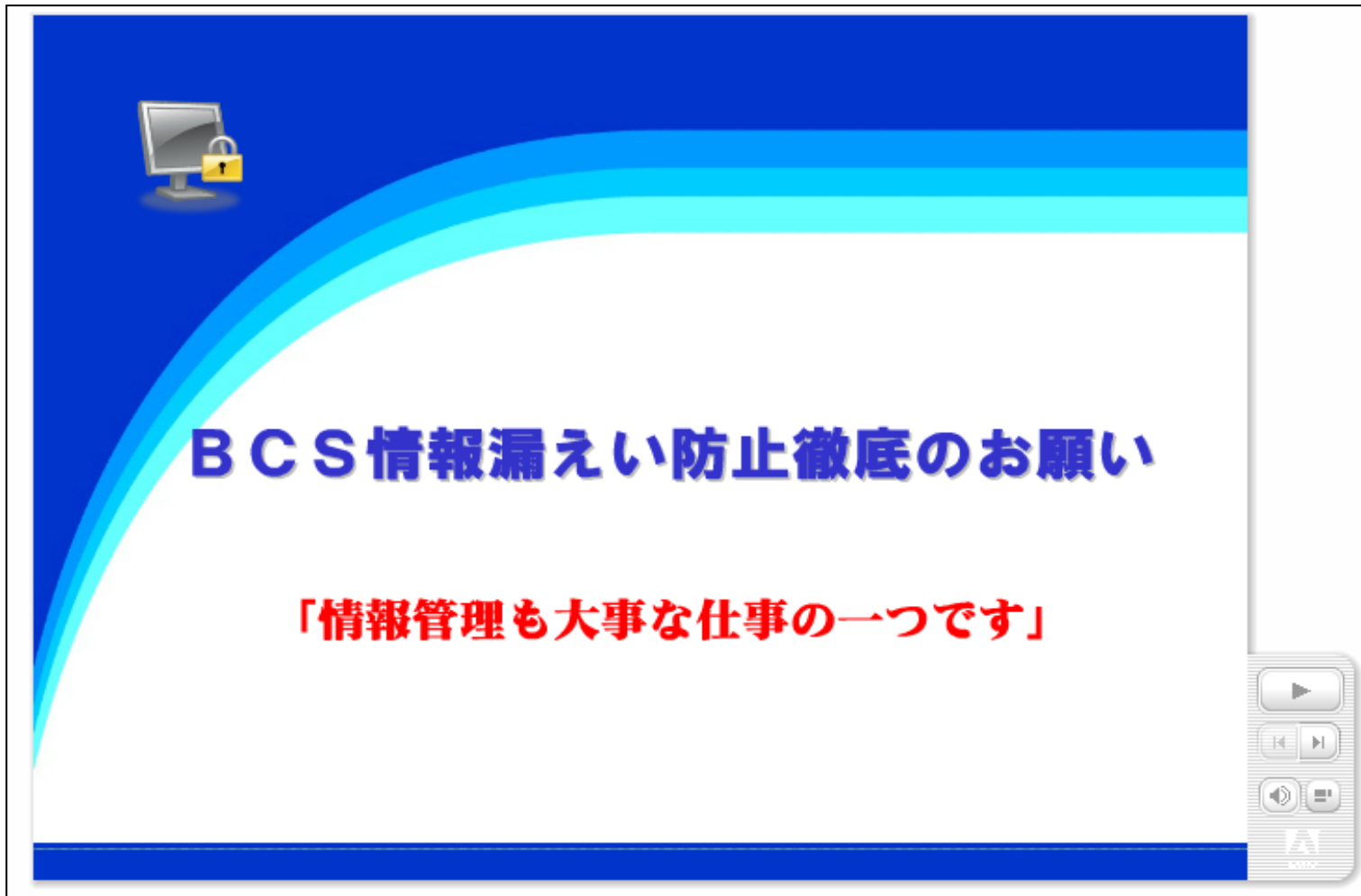
万が一にも、情報漏えい事故が発生した場合、また情報漏えい事故の恐れがあると判断した場合には、社員は直ちに自社の上司または担当者に報告してください。報告を受けた会社は、元請会社などの関係先に連絡してください。

情報漏えい防止対策について、この資料に書かれていることで分からないことがありましたら、当社社員にお尋ねください。

(2009.5.26 版)

○その他(セキュリティツールの紹介)

教育用動画 「情報漏えい防止徹底のお願い」



○その他(セキュリティツールの紹介)

現場用 情報セキュリティポスター

パソコンには重要情報が入っています
あなたのパソコンが
狙われています!



ワイヤーでPCを固定



保管時にはしっかり施錠

⚠ 保管管理の徹底
事務所荒らしによるパソコンの盗難が多発しています

🔒 パソコンはワイヤーで固定し、外部記憶媒体 (USB メモリー / CD 等) は決められた場所に保管し、施錠してください!

社団法人日本建設業連合会

情報は絶対に口外せず
確実に返却・破棄しましょう

情報
狙 われています!
Cybercrime

情報漏えい
一刀両断



社団法人日本建設業連合会



○その他(今後の取り組み)



業界標準の「セキュリティチェックリスト」作成

- アンケートを実施して、セキュリティレベルの把握
(次のセキュリティ対策へ)
- セキュリティチェックリストの運用を検討
(各社毎の運用の非効率化を解消するために)



「ガイドライン」「教育ツール」は、
日建連HP(→建築→IT推進部会)より、ダウンロードができます

ご静聴ありがとうございます

メンバー(会社名順)

高馬 洋一
津久井 啓介
鳥飼 裕之
中俣 一夫
丹治 弘典
葛原 徹
平井 明
豆腐谷 洋一

安藤ハザマ
大林組
奥村組
鹿島建設
清水建設
大成建設
大成建設
竹中工務店

上村 昌弘
長沼 秀明
小澤 敦
西牧 晋志
山口 正志
藤野 芳徳
仙波 幹徳
長谷 芳春

鉄建建設
戸田建設
飛島建設
西松建設
フジタ
前田建設工業
三井住友建設
三井住友建設