



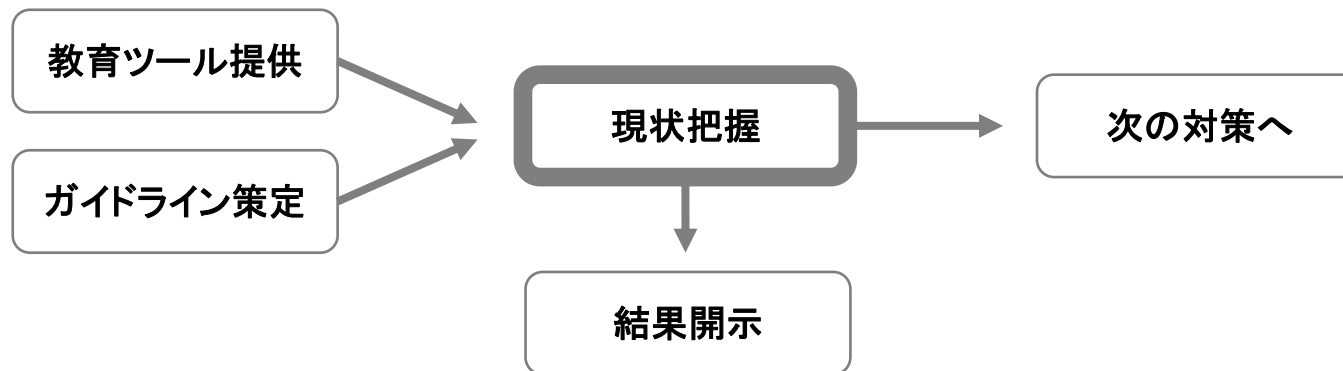
「協力会社における情報セキュリティについて」

- 1) 協力会社へのアンケート報告
- 2) 建設現場におけるガイドライン改定
- 3) 協力会社向け e-learning の展開

2015/2/17「建築のITセミナー」資料



【目的】



【実施概要】

時期	2014年5月1日 ～ 2014年6月15日
対象	情報セキュリティ専門部会委員会社(10社)の協力会社 依頼数 約8,000社(重複あり)、回答数 1,935社
方式	クラウドサービス利用 会社分類×3、ガイドライン等活用×6、 会社体制×6、セキュリティ対策×24、自由記述

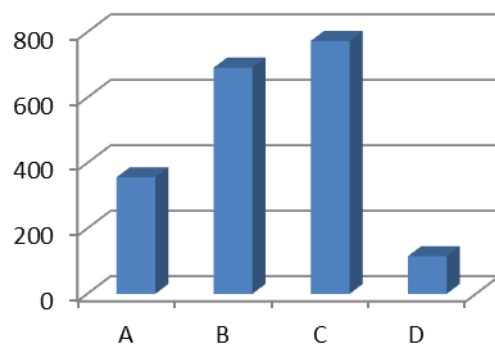


【アンケート結果】

会社分類

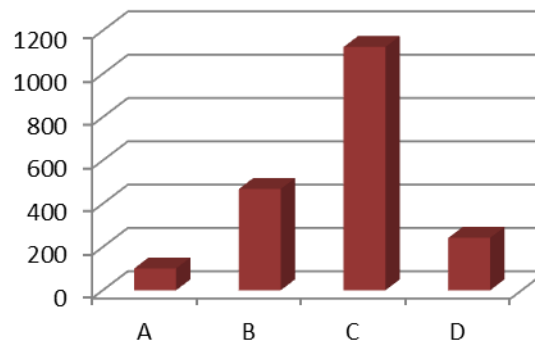
売上高

A 100 億 ～	356
B 100 億 未満	691
C 10 億 未満	773
D 1 億 未満	115



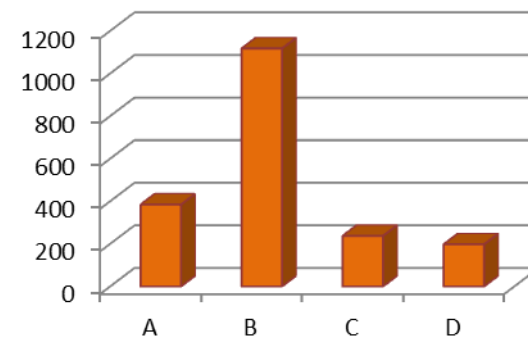
従業員

A 1,001 ～	101
B 101 ～	468
C 11 ～	1,124
D 1 ～	242



業種

A 土木	384
B 建築	1,117
C 設備	237
D その他	197



1) 協力会社へのアンケート報告

—まとめ方—



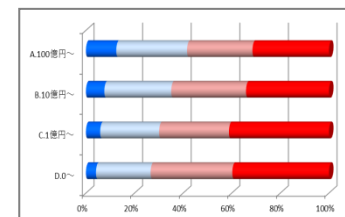
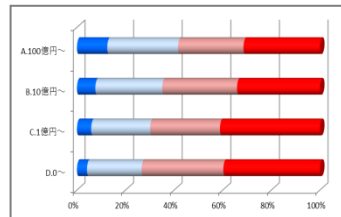
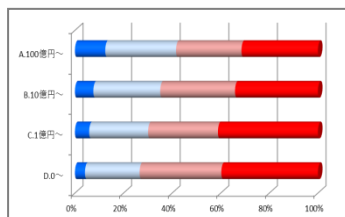
【アンケート結果】 会社分類毎にアンケート内容で傾向を表示(次頁以降)

ガイドライン等の活用

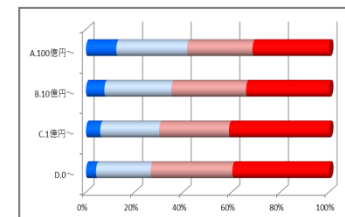
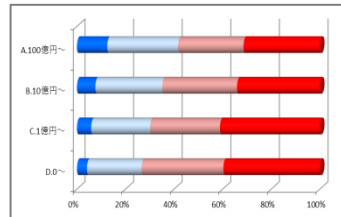
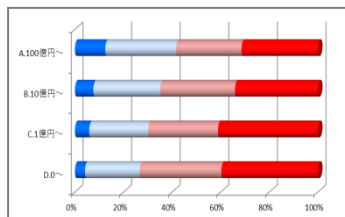
社内体制

個別対策

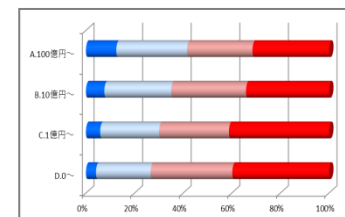
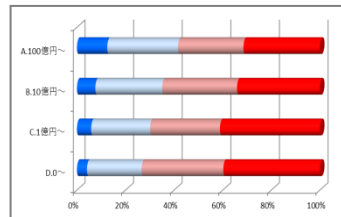
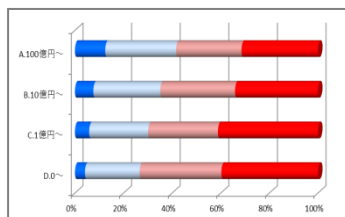
売上高



従業員



業 種





【アンケート結果】

ガイドライン等の活用 (全面活用) (一部活用) (未活用) (知らない)

①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) 2008/11 発行

②「情報漏えい防止徹底のお願い」パンフレット 2009/11 発行

③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】 2010/06 発行

④情報漏えい防止徹底のお願い～教育用ツール【動画】～ 2011/01 発行

⑤セキュリティポスター 2012/03 発行

⑥建設現場ネットワークの構築と運用ガイドライン 2013/08 発行

1) 協力会社へのアンケート報告 —売上高別・ガイドライン活用—

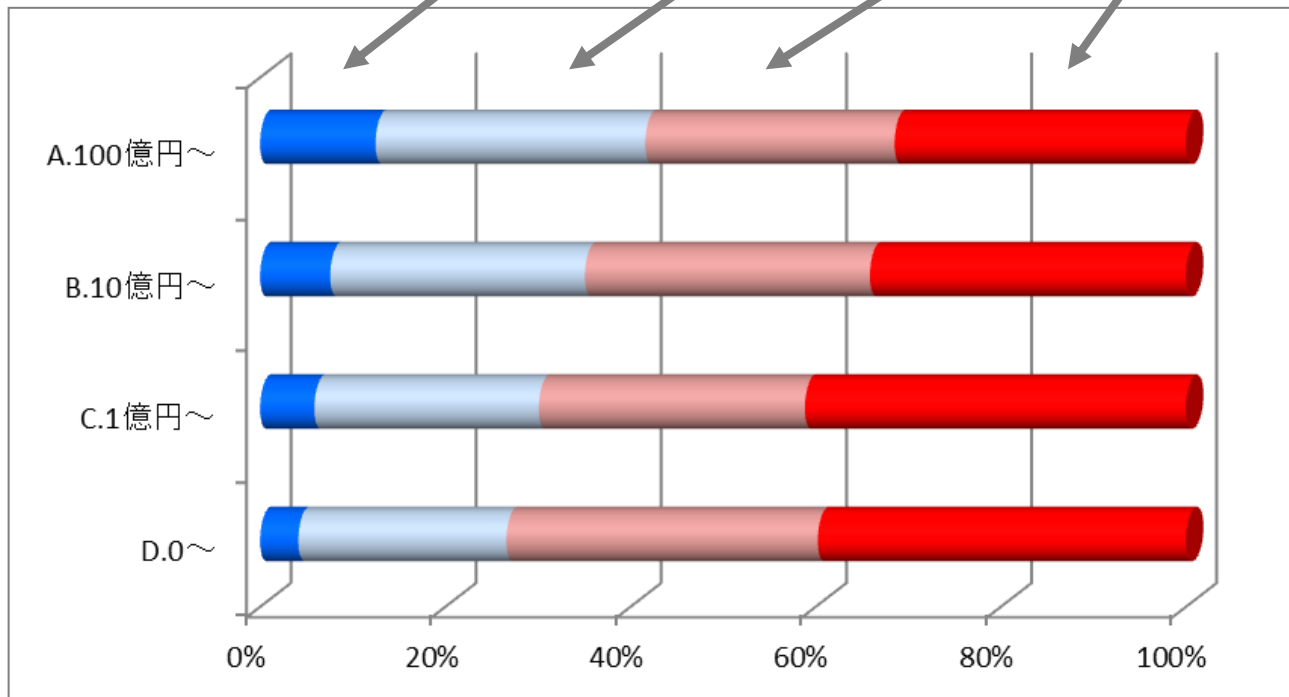


【アンケート結果】

ガイドライン等の活用

(全面活用) (一部活用) (未活用) (知らない)

売上高



1) 協力会社へのアンケート報告 —従業員別・ガイドライン活用—

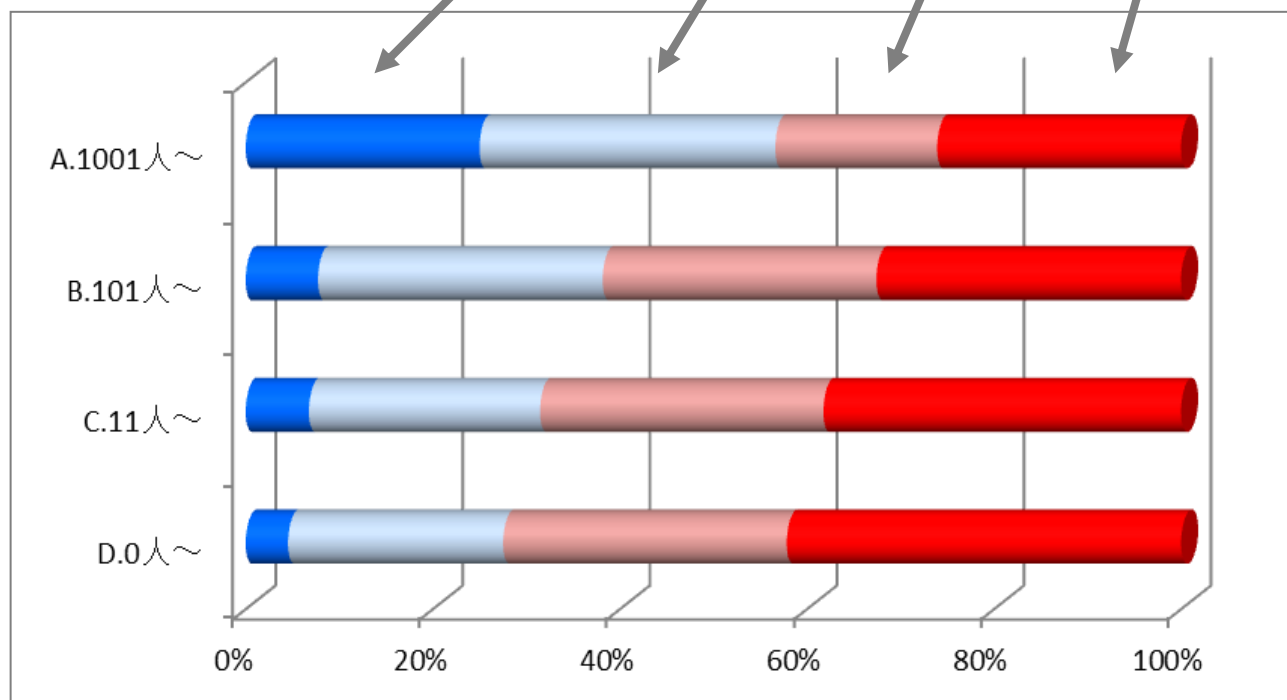


【アンケート結果】

ガイドライン等の活用

(全面活用) (一部活用) (未活用) (知らない)

従業員



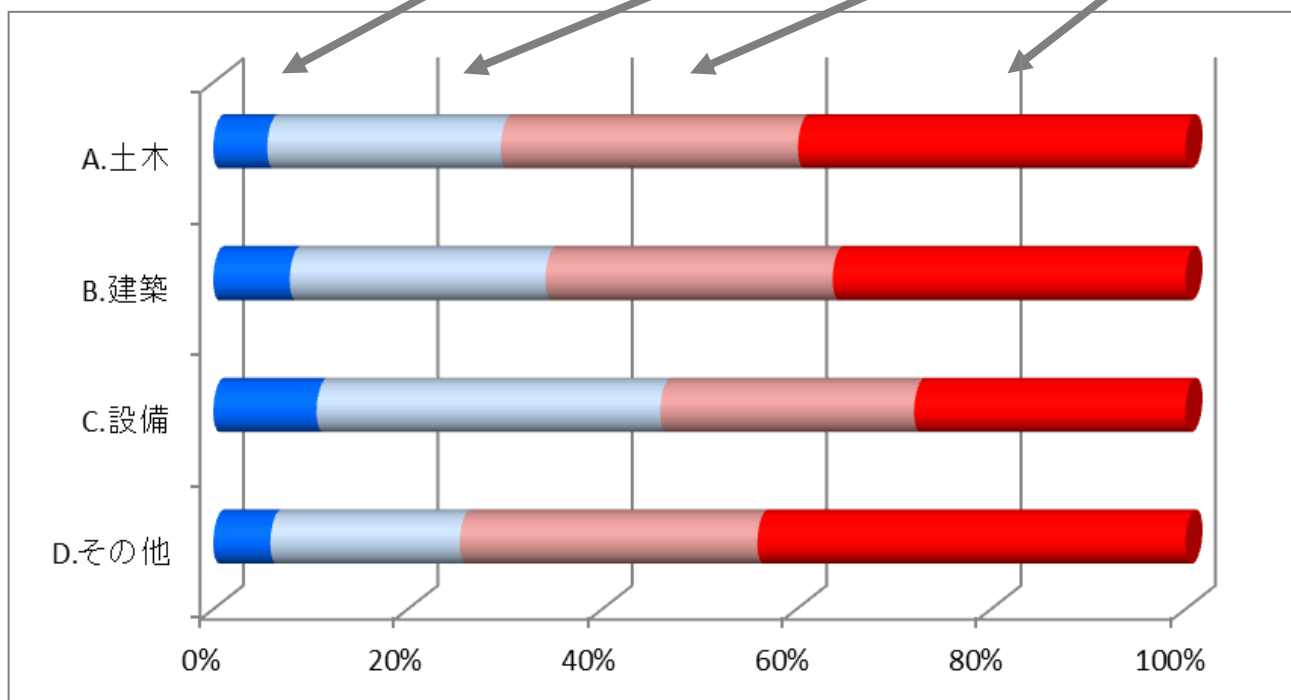


【アンケート結果】

ガイドライン等の活用

(全面活用) (一部活用) (未活用) (知らない)

業
種





【アンケート結果】

社内体制

(整備済)

(整備中)

(未整備)

①管理体制

- ・責任者、組織
- ・見直し

②事故発生時の対応

- ・対応手順、連絡体制

③情報セキュリティルール

- ・社内ルールの整備

④情報セキュリティ教育

- ・定期的な教育の実施

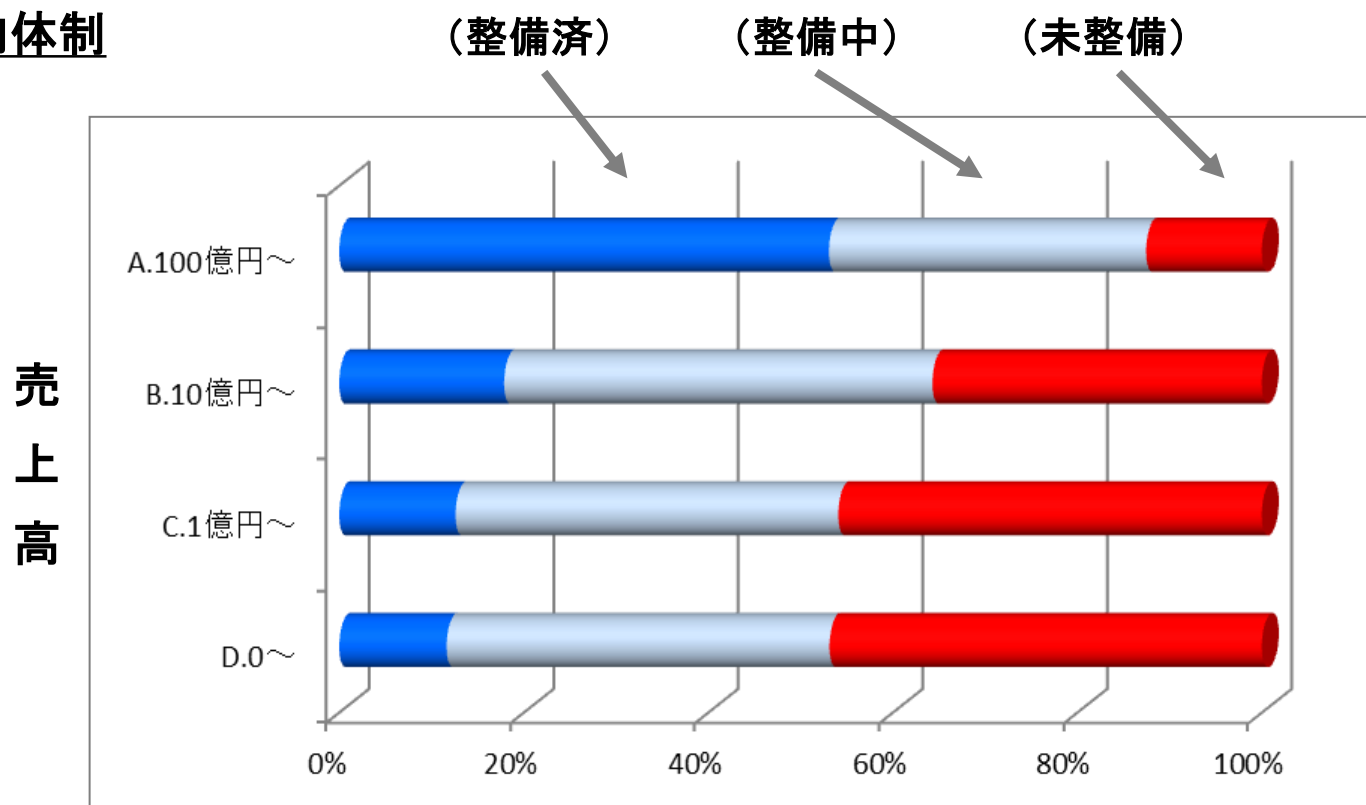
⑤再下請時の留意事項

- ・機密保持契約



【アンケート結果】

社内体制

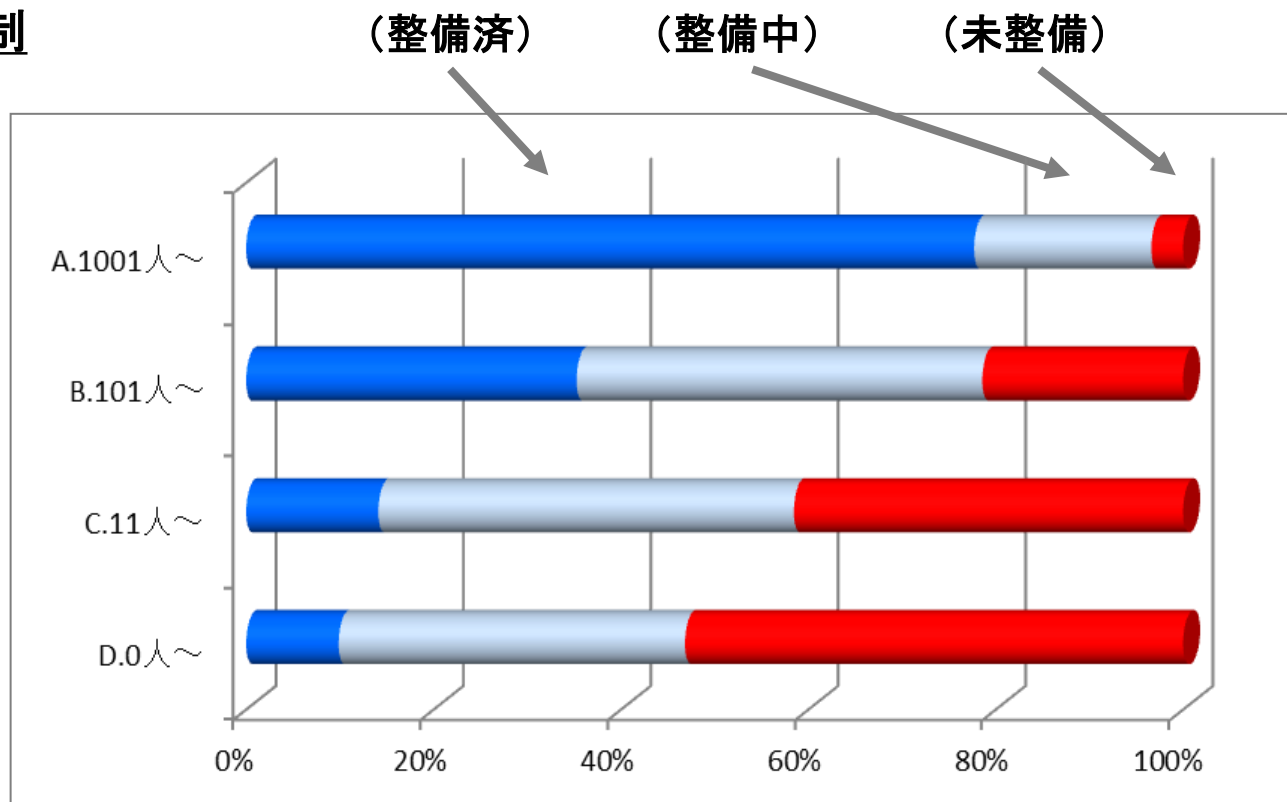




【アンケート結果】

社内体制

従業員

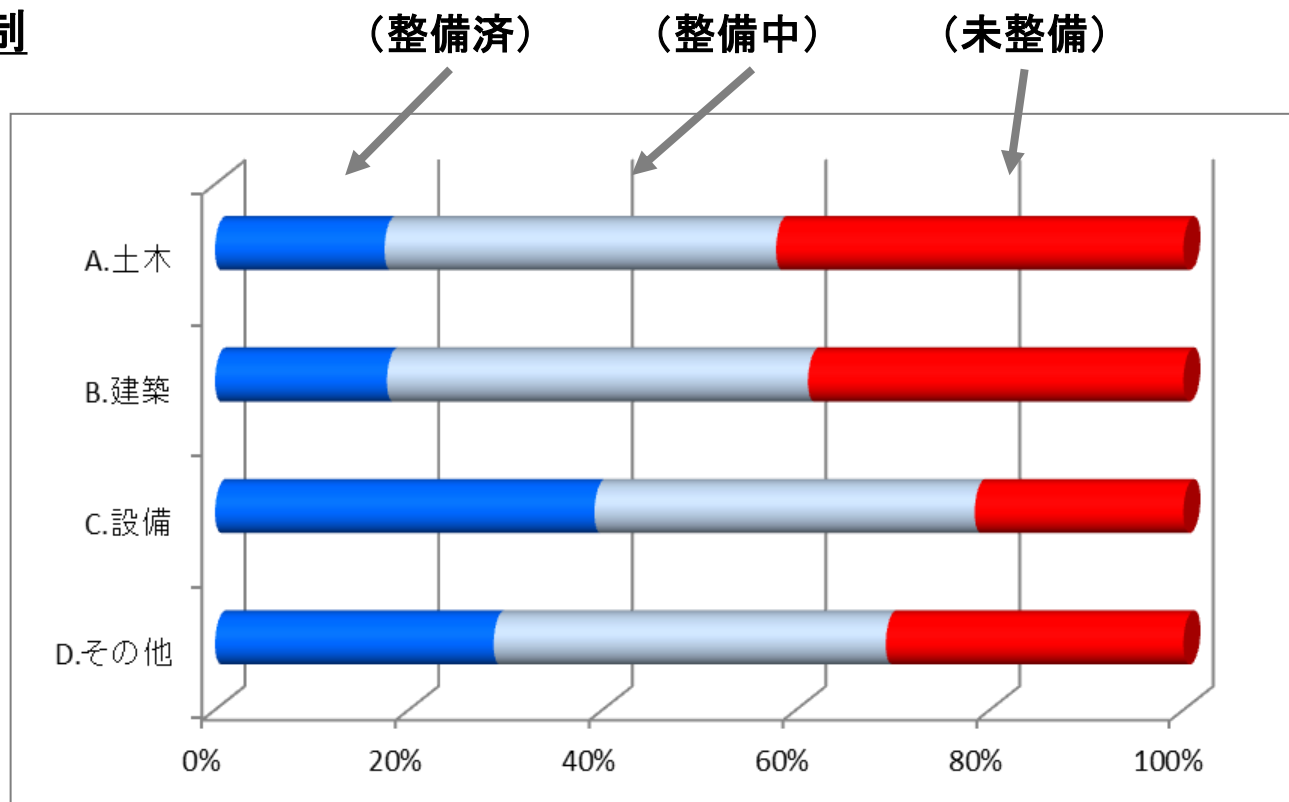




【アンケート結果】

社内体制

業種





【アンケート結果】

個別対策

(実施)

(一部実施)

(未実施)

①個人所有の取り扱い

④利用禁止ソフト
【ファイル交換】
【無許可導入】

⑧情報の取り扱い
【インターネット開示】
【最小限の複製】

②盗難・紛失対策
【パスワード管理】
【施錠管理】
【事務所】
【暗号化】
【社外持出対策】
(情報機器)
(紙)

⑤メールの注意事項
【添付ファイル対策】
【不信メール】

⑨情報の廃棄管理
【紙】
【データ】

③ウイルス対策
【ウイルス駆除ソフト】
【セキュリティパッチ】

⑥FAX・郵送等の注意

⑩個人情報保護

⑦データ交換
【情報漏えい対策】
【受渡し管理表】

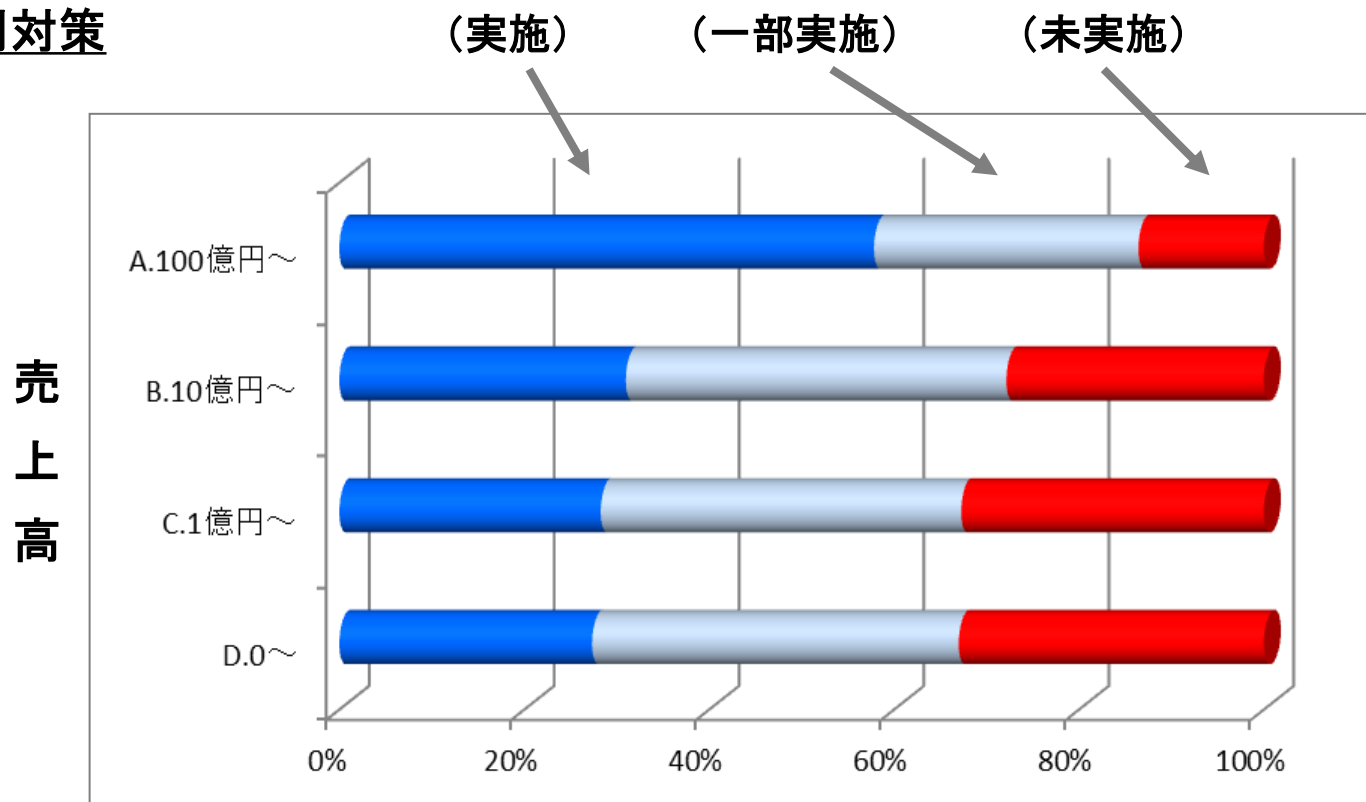
⑪ネットワーク

⑫バックアップ



【アンケート結果】

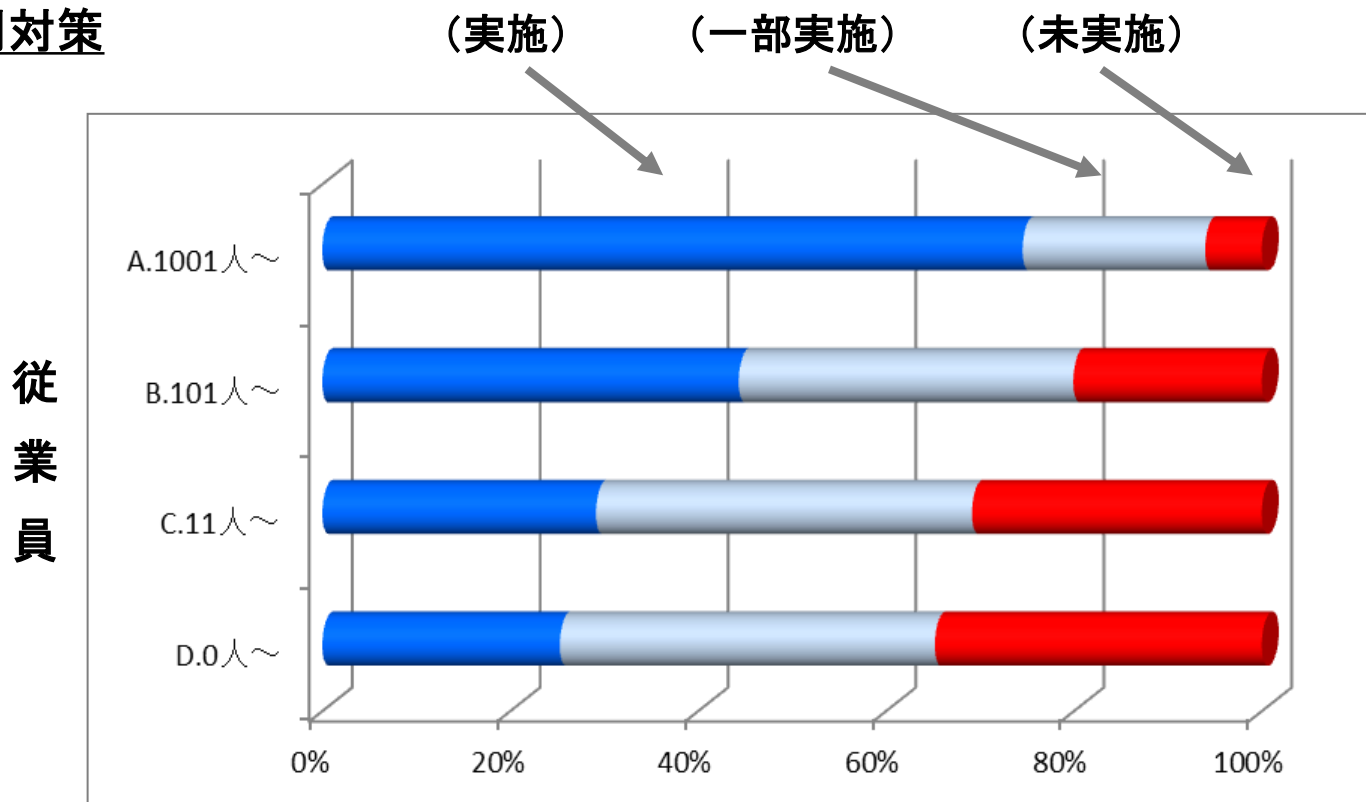
個別対策





【アンケート結果】

個別対策

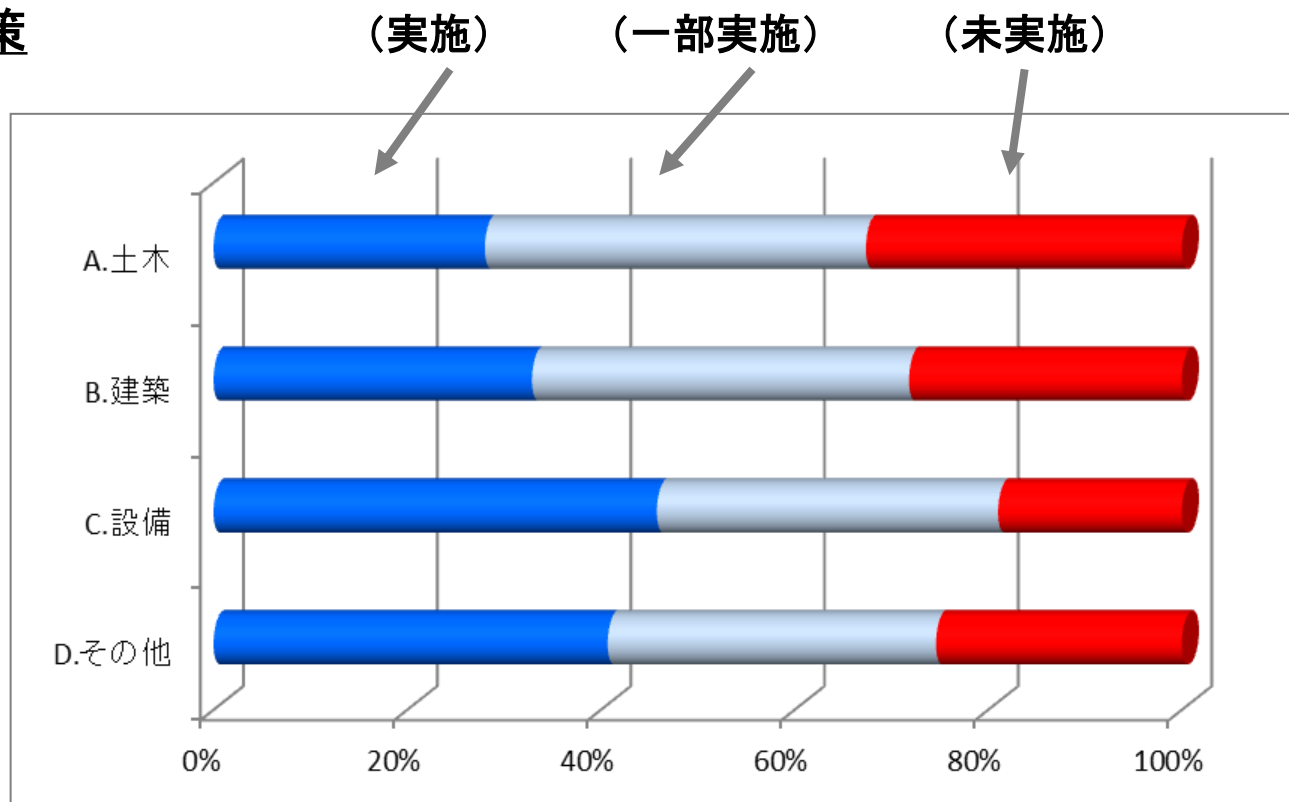




【アンケート結果】

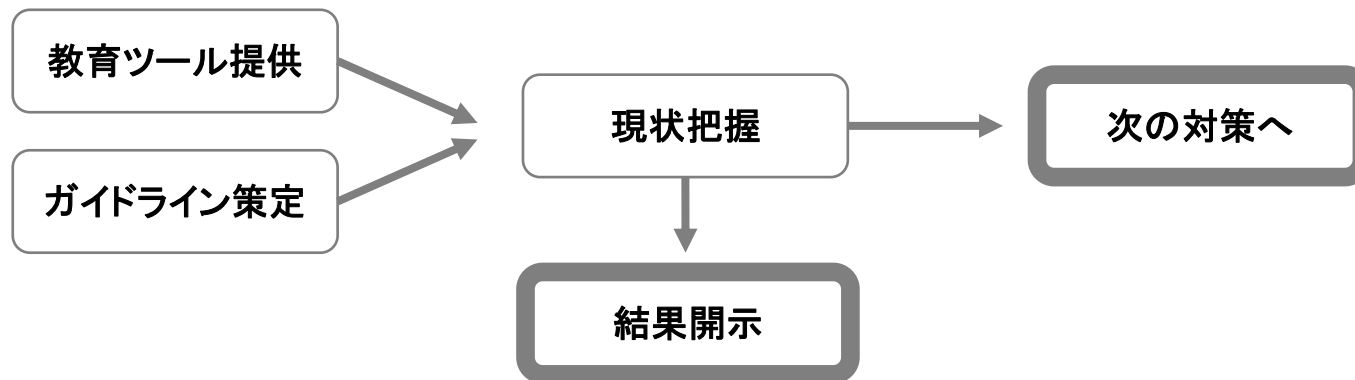
個別対策

業
種





【目的】

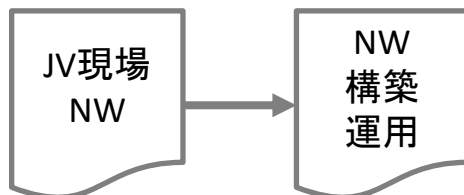


- ✓ アンケート依頼会社に対して、アンケート結果を開示
→ 自社の置かれている状況を認識してもらい、対策に役立ててもらう
- ✓ アンケート内容(チェックシート)の標準化
→ 元請企業毎のアンケートの統一に向けて(ガイドラインに盛り込む)
- ✓ アンケート回答(自由意見)の要望
→ e-learning の展開 (教育ツールがほしい)

2) 建設現場におけるガイドライン改定 ―既存ガイドライン―

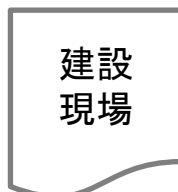


【これまで発行したガイドライン】



2013年11月

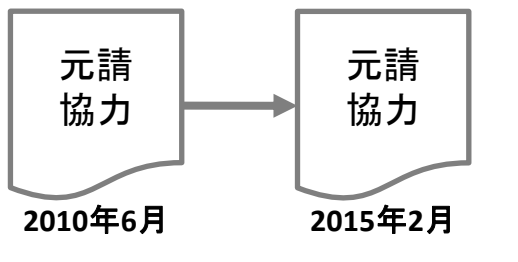
建設現場ネットワークの安全・安定した運用と
建設現場への容易な導入を目的



2008年11月

建設業特有の生産拠点である建設現場に焦点をあて、
情報セキュリティ事故発生防止に役立てる

今回の改訂範囲



2010年6月

2015年2月

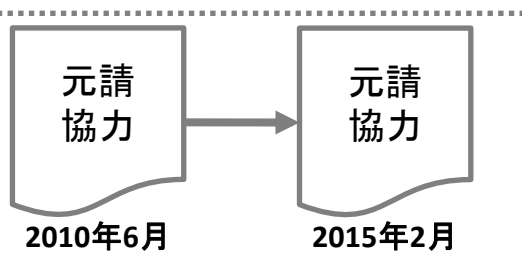
情報漏えい防止に焦点をあて、
元請会社、協力会社の実施事項をまとめる

2) 建設現場におけるガイドライン改定 ー改定のポイントー



【改定のポイント】

今回の改訂範囲



情報漏えい防止に焦点をあて、
元請会社、協力会社の実施事項をまとめる

Point !



「情報セキュリティチェックシート」を作成

→ 活用方法を解説し、セキュリティの維持・向上につなげる

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)第2版

→ 「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)」

建設現場における情報セキュリティガイドライン(協力会社編)第2版

→ 「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)」

2) 建設現場におけるガイドライン改定 –チェックシート(体制)–



【チェックシート】 (体制について:6問)

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)

記載日: 年 月 日

No.1～6は、できる限り経営層の方が直接回答して下さい。

No.	項目	チェック内容
		質問
1	管理体制	情報セキュリティを管理・推進するための責任者や社内体制・組織を整備していますか。
2		情報セキュリティ対策が守られていることを定期的(1回/年以上)に確認していますか。
3	事故発生時の対応	情報漏えい事故(情報機器の盗難・紛失、メール誤送信等)があった又は発見した場合の対応手順や連絡体制を整備するなど、事故があった場合の準備をしていますか。
4	情報セキュリティルール	情報セキュリティに関する社内ルールを策定するなど、情報セキュリティ対策の内容を明確にしていますか。
5	情報セキュリティ教育	従業員に対し情報セキュリティ教育を定期的(集合教育、eラーニング)し、意識付けを行っていますか。
6	再下請時の留意事項	再下請先との契約書に機密保持(守秘義務)項目を盛り込むなど、再下請先へ機密を守ることを求めていますか。

2) 建設現場におけるガイドライン改定－チェックシート(対策①)－



【チェックシート】（個別対策について:24問_1）

No.	項目	チェック内容
		質問
7	個人所有の取り扱い	会社として許可した以外の私有のパソコンやUSBメモリ、スマートフォン等を業務で使用することを禁止していますか。
8	盗難・紛失対策 【パスワード管理】	パソコンやUSBメモリ、スマートフォン等を利用するためのパスワードは、他者に推測されにくいものを設定し、外部に漏れることのないよう管理していますか。
9	盗難・紛失対策 【施錠管理】	情報機器の保管は、施錠等による盗難防止措置を講じ、第三者による不正な閲覧、持ち出し等を防止していますか。
10	盗難・紛失対策 【事務所】	執務室や作業場所への部外者の立ち入り禁止措置等警備に対して、対策を実施していますか。また機械警備等の事務所の防犯対策を強化していますか。
11	盗難・紛失対策 【暗号化】	情報機器に保管されている情報は、暗号化を設定していますか。
12	盗難・紛失対策 【社外持出対策(情報機器)】	電子データをパソコン、可搬記憶媒体に保存して外に持ち出す際は、暗号化、パスワードの設定など、データを保護するための措置を講じていますか。
13	盗難・紛失対策 【社外持出対策(紙)】	書面を外に持ち出す際は、紛失、置き忘れ、盗難等の事故を防止するための措置(ルールの策定等)を講じていますか。
14	ウイルス対策	業務で使用するパソコンやサーバには、ウィルス対策ソフトを導入し、パターンファイルを常に最新の状態に保っていますか。
15		業務で使用するパソコンやサーバ等には、定期的にソフトウェアのセキュリティパッチを適用していますか。

2) 建設現場におけるガイドライン改定ーチェックシート(対策②)ー



【チェックシート】（個別対策について:24問_2）

No.	項目	チェック内容
		質問
16	ソフトウェアの利用禁止	業務で使用するパソコンでWinnyなどのファイル交換ソフトの導入を禁止していますか。
17		個人の判断で勝手にソフトウェアを導入することを禁止していますか。
18	メールの注意事項	メールを送信する場合は、重要な添付ファイルには暗号化やパスワードを設定していますか。
19		不審なメール(送信元が不明等)を受信した時の対策をとっていますか。
20	FAX・郵送等の注意事項	FAX、郵送などにより送信・送付する場合は、誤発信等の事故への対策をとっていますか。
21	データ交換	社外とのデータ交換に伴う情報漏えい事故を防止するための措置をとっていますか。
22		預かった情報の受渡しを管理表を作って記録していますか。
23	情報の取り扱い	情報(写真、動画を含む)が第三者の目に触れるような行為(インターネットの掲示板・ブログへの書き込み、プライベートのメールへの記載・添付、その他の手段、方法による情報発信)を行わないようにしていますか。
24		複製は必要最小限の範囲に留めるなど、情報を工事等の目的以外で使用することを禁止していますか。

2) 建設現場におけるガイドライン改定－チェックシート(対策③)－



【チェックシート】（個別対策について:24問_3）

No.	項目	チェック内容
		質問
25	情報の廃棄管理【紙】	不要となった書面情報は、返却するか、あるいは裁断するなどにより判読できないよう処理したうえで廃棄していますか。
26	情報の廃棄管理【データ】	パソコン及び外部記憶媒体(USBメモリ、外付ハードディスク等)を廃棄する際は、データを読み出しできないように処理してから廃棄していますか。
27	個人情報保護	個人情報保護に関する対策をとっていますか。
28	再下請先への教育	再下請先に情報セキュリティ教育を実施していますか。
29	ネットワーク	日本建設業連合会発行のガイドライン(「建設現場ネットワークの構築と運用ガイドライン」等)に準拠して実施していますか。
30	バックアップ	重要情報のバックアップを定期的に行うなどのように、故障や誤操作、紛失などに備えて重要情報が消失しないような対策をしていますか。

Point !



重要事項を建設業界として標準化

→ 「誰もが同じ視点で」また「経年変化を把握」

3) 協力会社向け e-learning の展開 —目的・実施要領—



【目的】

セキュリティレベル向上のために

- ← 従事者1人1人の意識が大切
- ← 教育が必要

(協力会社)

簡易な教育ツールが欲しい

e-learning の展開

【実施概要】

クラウドサービスを利用

- ・個人が好きな時間に受講
- ・教育内容を簡単に作成
- ・作成が安価で可能
- ・回答状況を把握可能



【内容】

問1: 私有情報機器(パソコン、USBメモリ等)の取扱いについて

* 私有情報機器の取扱いで正しいのはどれですか

- ☒ 1. 自宅で仕事をするため、データをUSBメモリにコピーして持ち帰った
- ☐ 2. 自宅のパソコンを持ち込み、現場のネットワークに接続した
- ☐ 3. 自分で買ったスマートフォンは業務に使用しない

前へ

次へ

- ・ガイドラインの内容を選択形式で設問(5問)
- ・定期的に設問の入替えを予定

3) 協力会社向け e-learning の展開 ー 解説イメージ ー



問1: 解説

正解: 3. 自分で買ったスマートフォンは業務に使用しない

スマートフォンは手軽に利用できますが、パソコンと同様に情報セキュリティ対策が必要です。必ず、会社から貸与されたものを使用してください。

誤り: 1. 自宅で仕事をするため、データをUSBメモリにコピーして持ち帰った

自宅のパソコンや私有パソコンはセキュリティ対策が不十分になりがちです。業務には使わないでください。

誤り: 2. 自宅のパソコンを

自宅のパソコンや私有パソコンに業務情報を保管することにより、情報漏えいすることがあります。持ち込むかもしれません。私



・ガイドラインの図を引用し
わかりやすく解説

○その他(サイバーセキュリティ月間)

報道資料



平成 27 年 1 月 23 日
内閣サイバーセキュリティセンター (NISC)

2015 年「サイバーセキュリティ月間」の実施について

政府では、国民一人一人にサイバーセキュリティについての関心を高め、理解を深めていただくために、2月1日から3月18日までを「サイバーセキュリティ月間」※としています。期間中、政府機関はもとより、広く他の関係機関、団体等の協力の下に、サイバーセキュリティに関する普及啓発活動を集中的に推進します。

期間中は、産学官民の様々な主体により、全国各地でイベント開催やポスター掲示等の取組が行われます。また、政府としても、キックオフ・シンポジウムに始まり、一般向けの「サイバーセキュリティ・カフェ」、府省庁対抗による競技形式の事案対処訓練など、新たな取組を実施予定です。

さらに、インターネット上でも、「国民を守る情報セキュリティサイト」における日替わりコラムや普及啓発アニメの掲載、Yahoo!ニュースとの連携による意識調査などを実施します。

※「情報セキュリティ月間」は、今年度から「サイバーセキュリティ月間」に名称が変わりました。



○その他(サイバーセキュリティ月間)



1 「サイバーセキュリティ月間」の趣旨

巧妙さを増すサイバー攻撃、大規模な個人情報の流出など、国民生活に影響を及ぼすサイバーセキュリティの問題が多数報じられています。誰もが安心して情報通信技術の恩恵を享受するためには、国民の皆様一人一人がサイバーセキュリティについての関心を高め、これらの問題に対応していく必要があります。

サ

このため、政府では、サイバーセキュリティに関する普及啓発強化のため、2月1日から3月18日までを「サイバーセキュリティ月間」としています。

期間中、政府機関はもとより、広く他の関係機関、団体等の協力の下に、国民の皆様の幅広い参加を得た取組を集中的に推進することとしております。

○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」



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一つです

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。

工事に関係する

- ・ 図面、
- ・ 発注書（個人）
- ・ 建物の
- ・ 会社の
- ・ みなさん

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ました。ちゃんと設定すればWinny（ウニニー）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。

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。
（一般的なファイル交換ソフトは、以下の通りです）

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。

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す >>>

- ・ 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。万が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切断するなど、物理的に破壊する。
 - パソコン内の不要データを削除する。（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

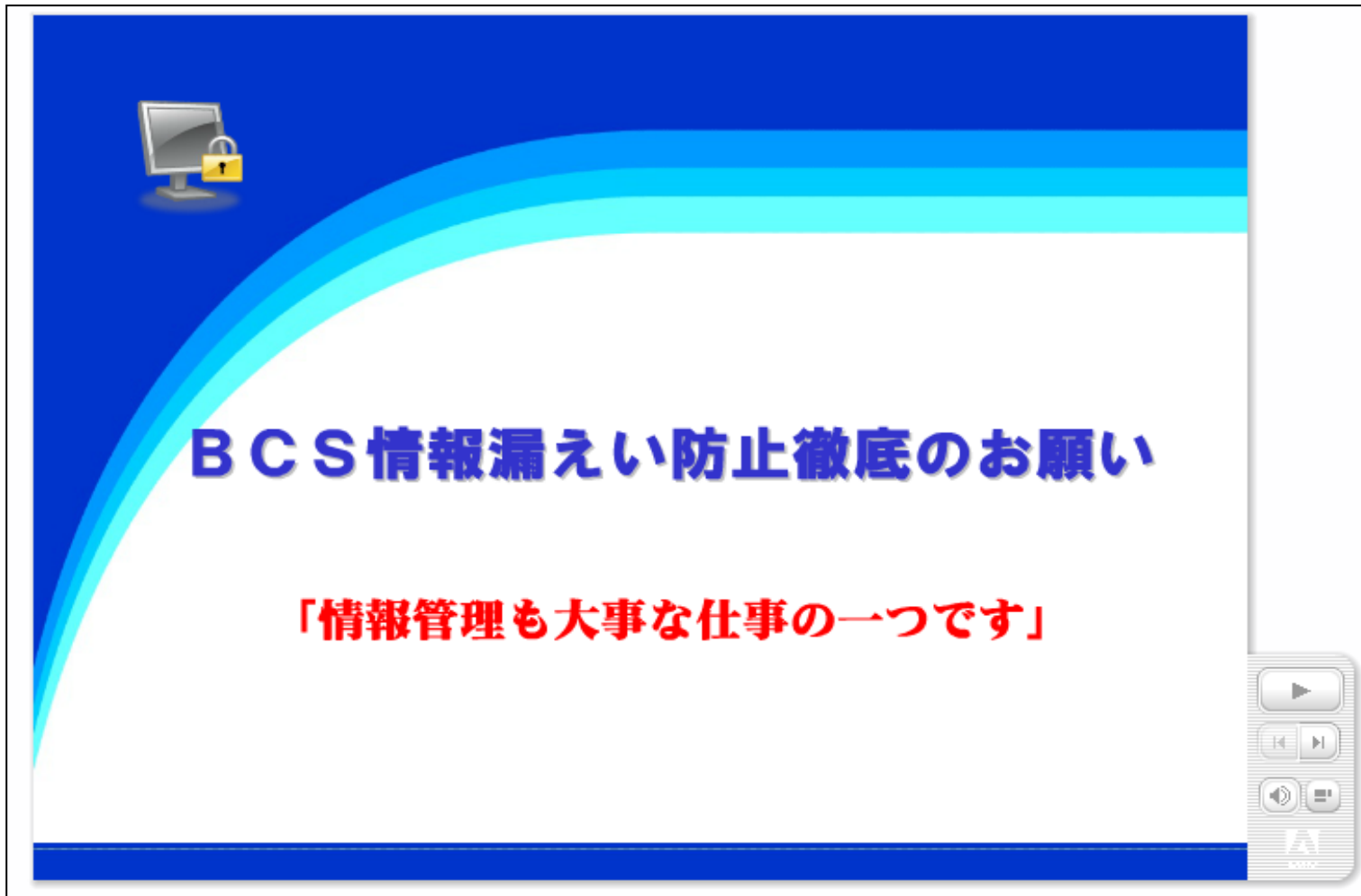
万が一にも、情報漏えい事故が発生した場合、また情報漏えい事故の恐れがあると判断した場合には、社員は直ちに貴社の上司または担当者に報告してください。報告を受けた会社は、元請会社などの関係先に連絡してまいります。

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





「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
中俣 一夫
石垣 順史
丹治 弘典
葛原 徹
平井 明

安藤ハザマ
大林組
鹿島建設
清水建設
清水建設
大成建設
大成建設

豆腐谷 洋一
長沼 秀明
山口 正志
藤野 芳徳
仙波 幹徳

竹中工務店
戸田建設
フジタ
前田建設工業
三井住友建設