

建設現場における情報セキュリティについて

- 1) サイバーセキュリティ月間
- 2) 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」
- 3) 教育用ツール

2016/2/26「建築のITセミナー」 資料

1)サイバーセキュリティ月間



建設現場における情報セキュリティについて

1)サイバーセキュリティ月間

2)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」

3)教育用ツール

1)サイバーセキュリティ月間



NISC内閣サイバーセキュリティセンターHPより

2月1日～3月18日は「サイバーセキュリティ月間」です。
普及啓発活動へご協力ください。

不審なメールによる情報漏えい被害や個人情報の流出など、生活に影響を及ぼすサイバーセキュリティに関する問題が多数報じられています。

誰もが安心してITの恩恵を享受するためには、国民一人ひとりが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。

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。

1)サイバーセキュリティ月間



NISC内閣サイバーセキュリティセンターHPより



スマートフォン利用者の方へ

特徴やリスクって？

スマートフォンは、利便性が高く、上手に利用すればとても有用なツールです。他方、

- ・国内外で幅広く導入されているOSを使用しているため、従来型の侵害手法と比較し、アタック対象になりやすい
- ・アプリケーションのインストールは許可されたアプリのみでも、悪意のあるアプリが混入している可能性がある
- ・ハードウェアの脆弱性や、OSの脆弱性などの特徴がありま



事例1：架空料金請求例

平成24年1月、動画を再生するアプリケーションを装って、を繰り返し表示させる不正なアプリケーションが確認されまは、動画サイト上で公開されており、利用者の電話番号やメ報を抜き取って、請求画面に表示する機能を備えていました

事例2：個人情報不正収集例

メールやソーシャル・ネットワーク・サービス（SNS）をアプリケーションに偽った不正なアプリケーションを紹介し、などの事例が確認されています。この不正なアプリケーションは、個人情報やメールアドレスなどの情報が外部に送信されてしまったなどのトラブルが発生

1)サイバーセキュリティ月間



IPA情報処理推進機構HPより

【情報セキュリティ10大脅威 2015】

- 1位「オンラインバンキングやクレジットカード情報の不正利用」
- 2位「内部不正による情報漏えい」
- 3位「標的型攻撃による諜報活動」
- 4位「ウェブサービスへの不正ログイン」
- 5位「ウェブサービスからの顧客情報の窃取」
- 6位「ハッカー集団によるサイバーテロ」
- 7位「ウェブサイトの改ざん」
- 8位「インターネット基盤技術の悪用」
- 9位「脆弱性公表に伴う攻撃の発生」
- 10位「悪意のあるスマートフォンアプリ」

1)サイバーセキュリティ月間



セキュリティ事故例 --- 1

新棟建設の工事中、発注者の旧棟会議室が見え、作業員がその会議の様子をSNSに投稿。発注者の指摘を受け、作業所内へのスマートデバイス持ち込み全面禁止となった

<point>

工事情報は口外しない(SNS、掲示版投稿禁止)

工事に直接関連しない情報でも、
SNS投稿により発注者が不快、不利益になる可能性がある

1)サイバーセキュリティ月間



セキュリティ事故例 --- 2

著名人の自宅リフォーム工事を請け負った会社の作業員が、現場の状況を家族に話し、家族が「〇〇さん家の台所はこんな風だったらしい」とSNSに投稿

<point>

工事情報は口外しない(SNS、掲示版投稿禁止)

業務で知りえた情報を家族や友人に話した場合、間接的に外部に漏れる可能性がある

1) サイバーセキュリティ月間



セキュリティ事故例 --- 3

メーリングリスト(ML)に顧客のアドレスが含まれており、送信者がそれに気づかず不適切なメールを送信した

<point>

メールの宛先は再確認した後に送付する

MLは、誰が対象になっているか確認して利用する
MLのメンバーは、目的に合った者だけに限定し、メンバーに変更があれば速やかに変更する

1) サイバーセキュリティ月間



セキュリティ事故例 --- 4

メール送信時にある職員が関係者以外のアドレスを誤って追加し、別の職員がそれに気づかず、関係者外秘の書類を全員へ返信してしまった

<point>

メールの宛先は再確認した後に送付する

「全員に返信」する場合は、とくにCCなどのアドレスをよく確認する

1) サイバーセキュリティ月間



セキュリティ事故例 --- 5

雨宿りで一時的にタブレット端末の入っている手荷物を付近に置いたが、そのまま置き忘れてしまった。すぐに戻ったが盗難した

<point>

情報端末は、一時的でも手放さない

(万が一に備え)

工事情報データは可能な限り保存しない

パスコードを設定する(推測されないものを)

1) サイバーセキュリティ月間



セキュリティ事故例 --- 6

車上荒らしにより、タブレットを紛失した。タブレット内には顧客の個人情報(氏名、住所、電話番号)が保存されていた

<point>

情報端末は、一時的でも手放さない(施錠した車内も不可)

(万が一に備え)

工事情報データは可能な限り保存しない

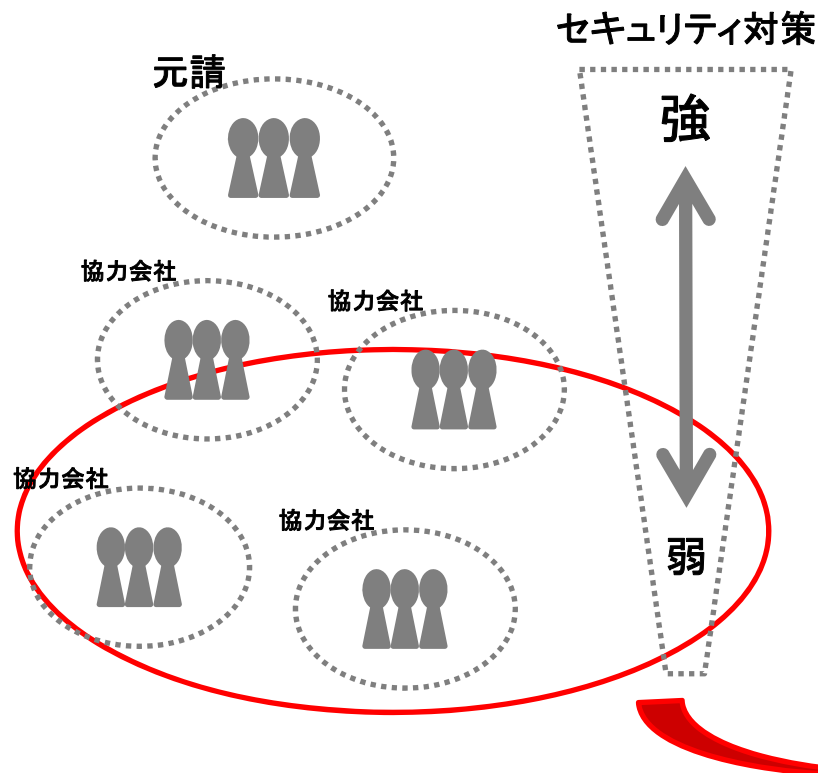
パスコードを設定する(推測されないものを)

1)サイバーセキュリティ月間



日建連 今年度の取り組み

ー「建設現場」特有の課題ー



【情報セキュリティ10大脅威 2015】

- 1位「オンラインバンキングやクレジットカード情報の不正利用」
- 2位「内部不正による情報漏えい」
- 3位「標的型攻撃による諜報活動」
- 4位「ウェブサービスへの不正ログイン」
- 5位「ウェブサービスからの顧客情報の窃取」
- 6位「ハッカー集団によるサイバーテロ」
- 7位「ウェブサイトの改ざん」
- 8位「インターネット基盤技術の悪用」
- 9位「脆弱性公表に伴う攻撃の発生」
- 10位「悪意のあるスマートフォンアプリ」

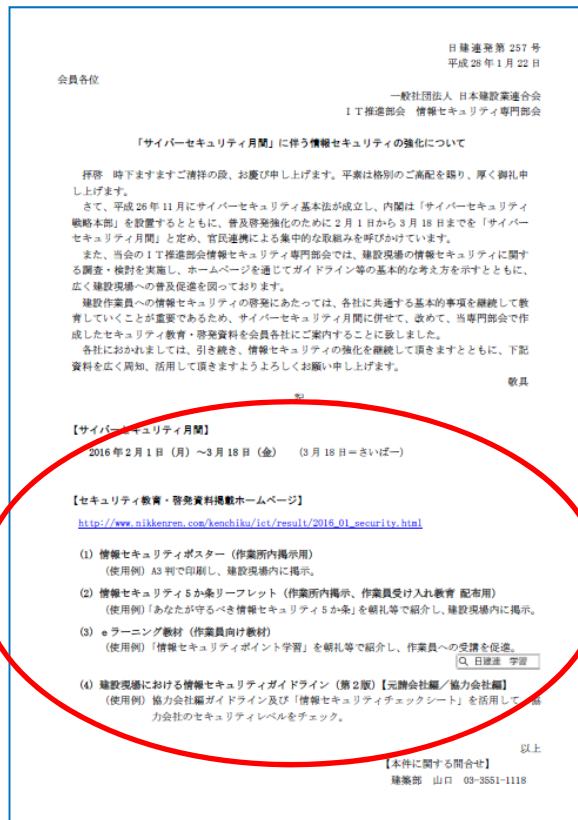
- ・作業員を対象に
- ・「情報漏えい」に焦点をあてる
(悪意の有無によらず)

1)サイバーセキュリティ月間



日建連 今年度の取り組み

会員会社への協力依頼(2015/1/22発信)



下記ツール類の活用を呼びかけ

- 1) セキュリティポスター
- 2) リーフレット(情報セキュリティ5ヶ条)
- 3) eラーニング教材
- 4) チェックリスト(ガイドラインより)

2)「セキュリティガイドライン」



建設現場における情報セキュリティについて

1) サイバーセキュリティ月間

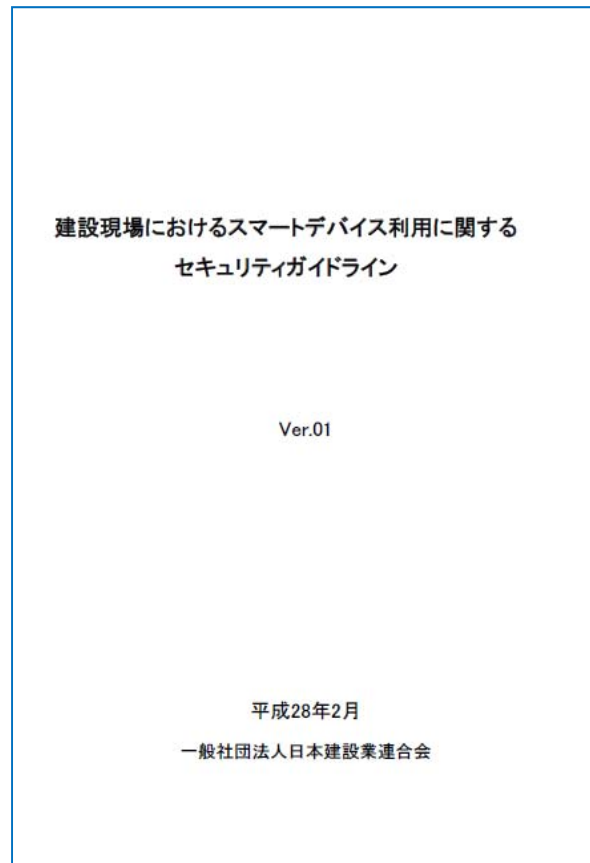
2) 建設現場における
「スマートデバイス利用に関するセキュリティガイドライン」

3) 教育用ツール

2)「セキュリティガイドライン」



「建設業における 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」発行



「はじめに」より抜粋

どこでも持ち歩けるスマートデバイスが進化し、建設現場の生産性向上などに役立つツールとして活用が始まっています。

しかし、情報漏えい事件・事故の発生源として、スマートフォン・タブレット等に起因するものが拡大しています。

SNSの特に写真や動画の投稿サイトが手軽に利用できるようになり、機密にすべき情報を安易に投稿して情報漏えい事件や自己が多数発生し、社会問題となっています。

2)「セキュリティガイドライン」

添付教育 A3版



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

～情報漏えい事故防止の徹底のお願い～

★スマートデバイスの紛失やSNSの投稿による
情報漏えい対策のポイントをまとめています。

解説)スマートデバイスは、スマートフォン、タブレット等を対象としています。
解説)SNSとは、ツイッターやLINE、Facebook等を対象としています。

○「工事情報」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つきます。

○もし、あなたの過失で「工事情報」が漏れてしまったら

万が一「工事情報」が漏れれば、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。
- 会社が信用を失い、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

●スマートデバイス利用に関する【5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いきましょう。

- ①スマートデバイスは、「許可なく」業務に使わない。
- ②情報を持出す時は「盗難・紛失対策」を行う。
- ③必ず「パスワード」を設定する。
- ④必ず「ウイルス対策ソフト」を入れる。
- ⑤工事情報をSNSに投稿することは「禁止」とする。

①スマートデバイスは、「許可なく」業務に使わない。

- スマートデバイスを、電話として利用することは問題ない。
- スマートデバイスにおいて、電話以外の機能(カメラ機能、メール機能、インターネット閲覧機能等)を業務で利用する場合は、作業所長の許可を必要とする。
- 業務で利用した工事情報を、業務の目的を達した以降も保存することは禁止とする。

②情報を持出す時は「盗難・紛失対策」を行う。

- スマートデバイス内に保存されている工事関連情報(写真やファイル)を必要以上に作業所から持ち出さない。
- スマートデバイスや外部記憶媒体を持ち出す場合には、盗難・紛失時の情報漏えいを防ぐため、暗号化やパスワード設定などを行う。
- 置き忘れによる紛失を防ぐため、職場の外では肌身離さないよう注意する。
- 盗難による紛失を防ぐため、電車の網棚に置いたり、車中に放置しない。



③必ず「パスワード」を設定する。

- スマートデバイスの盗難や不正利用の対策として、「必ずログインのパスワード(パスコード)」を設定する。
- パスワードは、1234や5555等の単純な数字の組合せや誕生日等の(推測されやすい)値は使わない。
- パスワードは、制限のない限り(英数混在の8文字以上)を推奨します。
- パスワードは、他人に漏れないように管理する。
- パスワードは、[複数回間違えたら内部のデータを初期化]する設定がある場合は機能を有効にする。



④必ず「ウイルス対策ソフト」を入れる。

- ウイルスによる情報漏えいを防ぐため、ウイルス対策ソフトを必ず入れる。
- 日々発生するウイルスに対応するため、ウイルス対策ソフトは、常に最新の状態にする。



⑤工事情報をSNSに投稿することは「禁止」とする。

- SNSの投稿により、情報が不特定多数に公開されますので、建物の内容(写真を含め)を、無断でSNSに投稿することや、作業所の内外や作業所周辺の写真など工事に関連しない情報でも、それをSNSに投稿することは、発注者に不利益となったり、発注者が不快に感じたりする可能性があります。



- 発注者に不利益となる投稿を行った場合、建設業全体の信頼を失うことにもなりかねません。
- また、発注者が個人の場合、プライバシー侵害の問題となりますので、注意してください。
- 家族や友人に対しても、工事情報をSNSに投稿させないように、注意してください。

例) ある発注者から依頼を受けた新棟建設の工事中、旧棟の会議室が見えたので、作業員がその会議の状況をSNSに書き込んだ。
旅館の増築工事中、「この旅館は土曜日ののに客がいっぱい」と掲示板に書き込んだ。

(2016.02.26 版)

■参考

総務省の国民のための情報セキュリティサイト
日建連の建設現場における情報セキュリティガイドライン(第2版)[元請会社編/協力会社編]
独立行政法人 情報処理推進機構の中小企業の情報セキュリティ対策ガイドライン
■不明な点は、会社担当者にお問い合わせ下さい。

2)「セキュリティガイドライン」



— 構成 —

はじめに

1. 目的
2. 対象者と対象物
3. 基本的な考え方
4. 利用許可した場合の実施事項
5. 建設現場での管理方法

作業所長へ

「協力会社の社員」
及び「作業員」への
「指導」「教育」に
活用していただきたい

— 添付資料 —

- ・「情報セキュリティ教育資料」
(協力会社のみなさんへ)
- ・「スマートデバイス持込・利用許可申請書」

2)「セキュリティガイドライン」



基本的な考え方

- (1) 建設現場に持ち込むスマートデバイスにおいて、電話以外の機能(カメラ機能、メール機能、インターネット閲覧機能等)を業務で利用する場合は、作業所長の許可を必要とする。
- (2) 作業所長が電話以外の機能での利用を許可する場合は、「4.利用を許可した場合の実施事項」と以下の「禁止事項」を遵守させる。
- (3) 施主・事業主からの要求または建設現場特有の事情により、スマートデバイスの建設現場への持ち込みを全面的に禁止するなどの現場特有の事情がある場合は、それに即した利用ルールを策定し遵守させる。

【禁止事項】

- ① 建設現場で撮影した写真や知りえた情報をSNS等(ツイッターやLINE、Facebook等)に投稿することは禁止する。
- ② スマートデバイスの電話以外の機能(カメラ機能、メール機能、インターネット閲覧機能等)を業務で利用したことによって、スマートデバイス内に保存された工事情報(例えば写真データ)を、業務が完了した後も保存し続けることを禁止する。
業務完了後はスマートデバイス内に保存された工事情報を速やかに削除するよう指導すること。

3) 教育用ツール



建設現場における情報セキュリティについて

1) サイバーセキュリティ月間

2) 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」

3) 教育用ツール

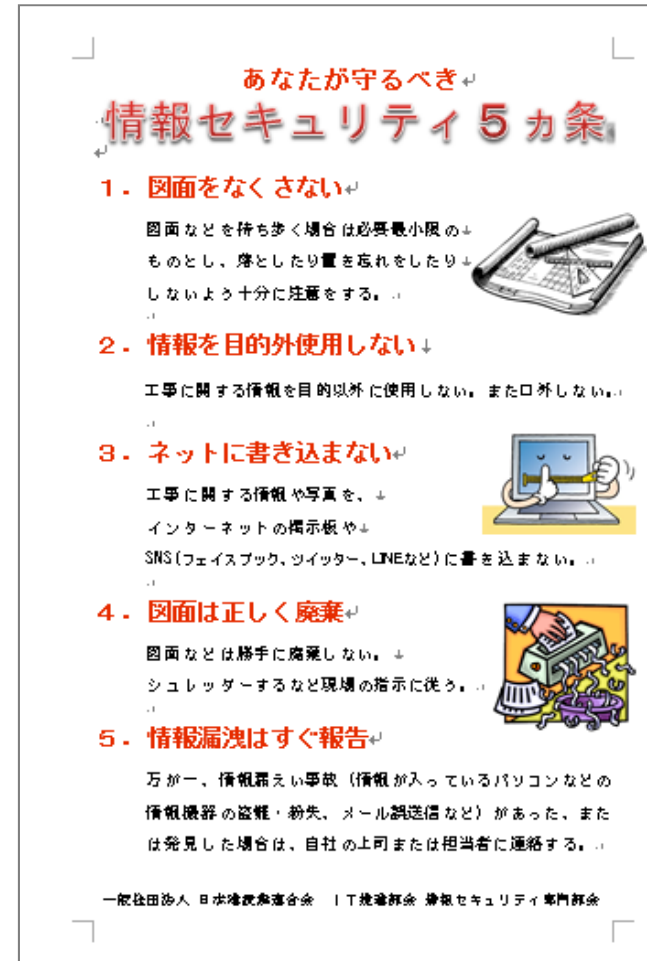
3) 教育用ツール



○ セキュリティポスター



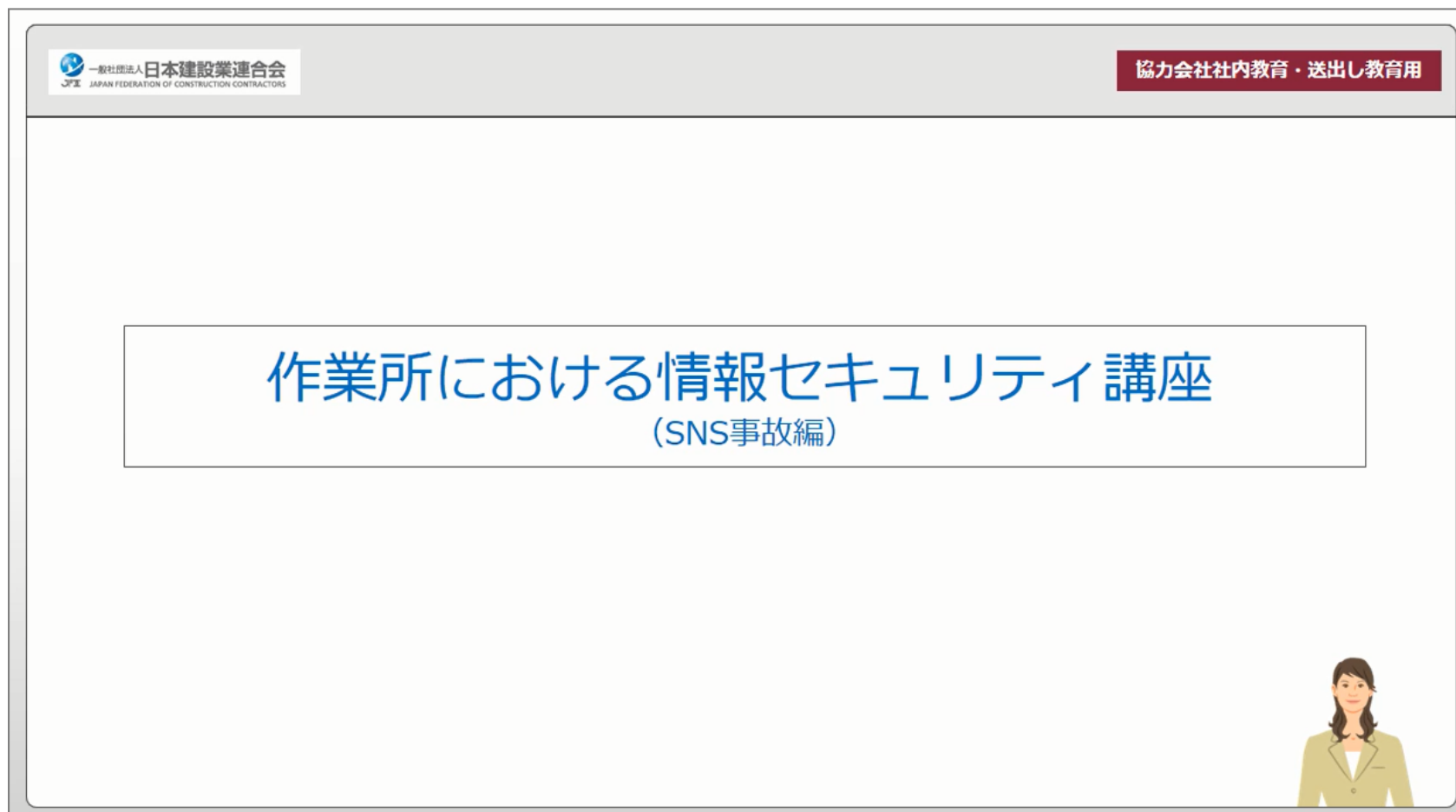
○ リーフレット



3) 教育用ツール



○ 教育用動画



3) 教育用ツール



○ eラーニング教材

Q 日建連 学習

e-learning(情報セキュリティポイント学習)の実施について

2015/10 Ver2 公開
2015/02 公開

2014年5月～6月に「情報セキュリティに関するアンケート」を実施したところ、情報セキュリティをどのように学んだらよいのかわからないので、勉強をするためのツールを提供してほしいとの意見が多く寄せられました。
そこで、いつでも好きな時間に手軽に勉強するためのツールとして、情報セキュリティe-learningを提供することとしました。
日常の情報セキュリティ対策の確認等にご活用いただき、より情報セキュリティに関する知識を深めて頂ければ幸いです。

[情報セキュリティポイント学習へ Ver2 \(2015/10\)](#)

[情報セキュリティポイント学習へ \(2015/02\)](#)

問2:「情報」保管について

* 情報の保管について、間違った対応はどれですか

- ☐ 1. 情報および情報機器の保管に関する会社のルールを定め、遵守する
- ☐ 2. 元請会社や取引先から預かった情報は管理台帳等に記載のうえ、厳重に管理する
- ☒ 3. 業務が終了した後も、

問2:解説

正解:3. 業務が終了した後も、参照する可能性のある情報はパソコンの中に保存していつでも参照できるようにしている

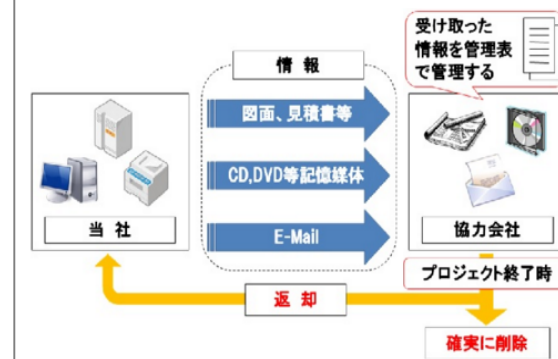
情報の保管として間違った対応です。業務が終了した時点で、元請会社や取引先から預かった情報は必ず返却、または、読めないようにした上で廃棄しなくてはなりません。

誤り:1. 情報および情報機器の保管に関する会社のルールを定め、遵守する

情報の保管として、正しい対応です。情報や情報機器の授受に関する会社のルール定め、遵守してください。

誤り:3. 元請会社や取引先から預かった情報は管理台帳等に記載のうえ、厳重に管理する

情報の保管方法として正しい対応です。預かった情報は管理台帳等に記載のうえ、厳重に管理してください。



3)教育用ツール(既存)



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。

工事に関係する方へ

- ・ 図面、書類
- ・ 発注書（個人）
- ・ 建物の写真
- ・ 会社の個人情報
- ・ みなさんの秘密

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て、ちゃんと設定すればWinny（ウニ）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。
- ・ パソコンを電卓に置き忘れたら、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。

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。

「情報」を守るための9つのポイント

ポイント5 ウィ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、ウィルスを検知・駆除するためのウィ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）
- ・ ウィルス対策ソフトは、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ろ。
 - 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」が漏れいしてしまったら

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、社員は直ちに会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。

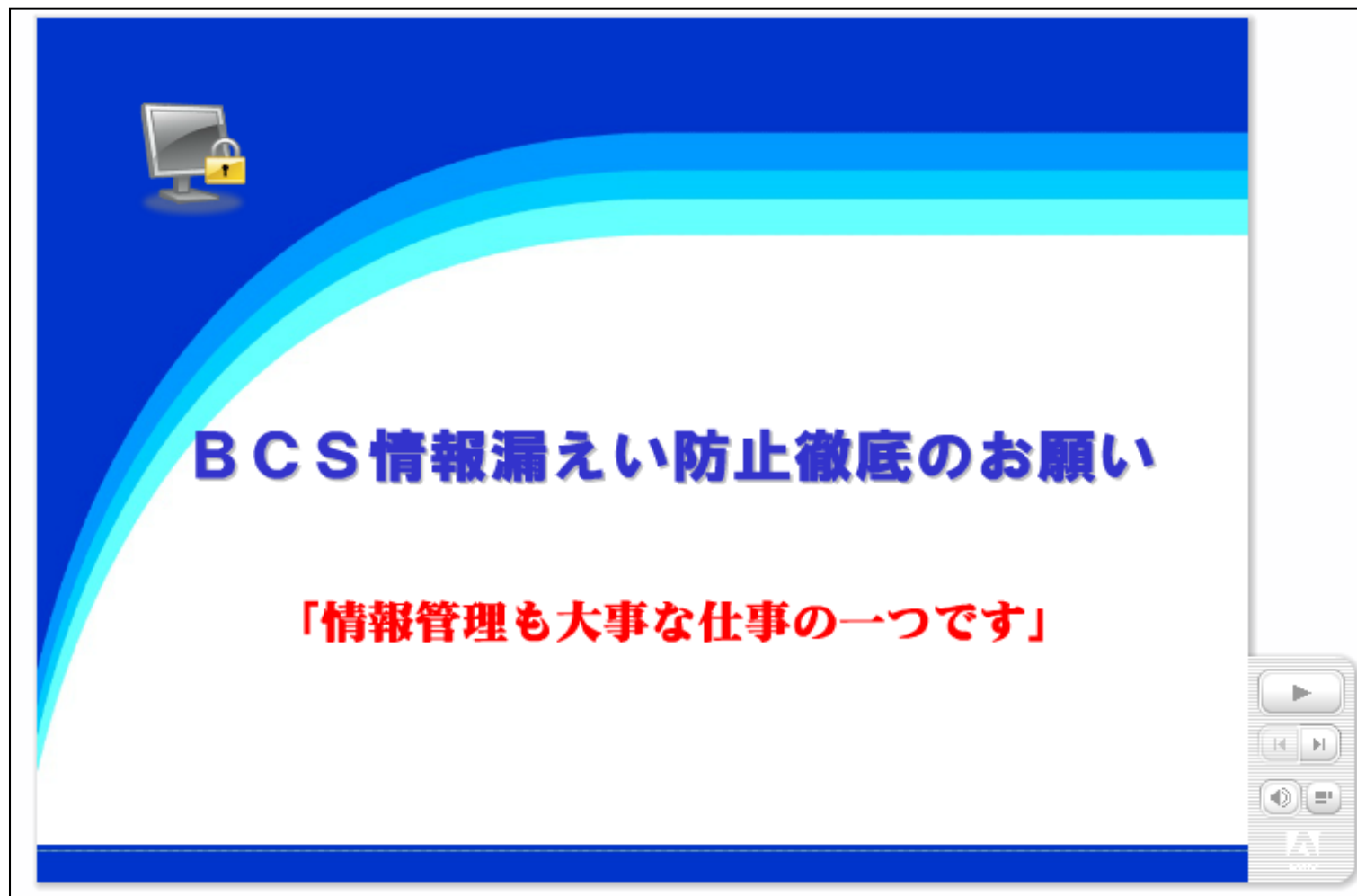
情報漏えい防止対策について、この資料に書かれていることで分からないことがありましたら、当社社員にお尋ねください。

(2009.5.26 版)

3) 教育用ツール(既存)



教育用動画 「情報漏えい防止徹底のお願い」



3) 教育用ツール(既存)

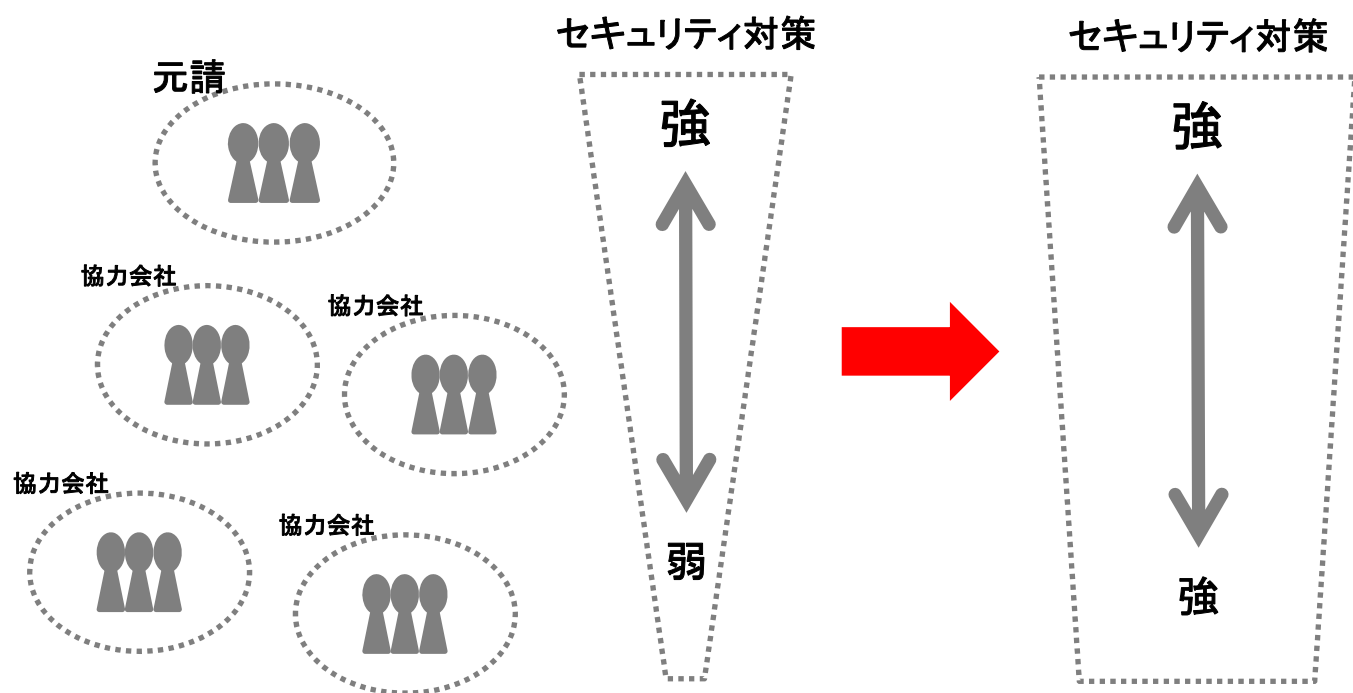


現場用 情報セキュリティポスター





今後も、建設業のセキュリティレベル向上に
取組んでまいります



ご協力、ご支援をお願いします

「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
大塚 暁
石垣 順史
葛原 徹
豆腐谷 洋一

安藤ハザマ
大林組
鹿島建設
清水建設
大成建設
竹中工務店

平峯 元晴
長沼 秀明
山口 正志
藤野 芳徳
仙波 幹徳

東急建設
戸田建設
フジタ
前田建設工業
三井住友建設