建設現場の
情報セキュリティガイドライン(概要)

(社) 建築業協会　IT推進部会
情報基盤セキュリティ専門部会

平成19年5月16日

■概要

- **何故セキュリティガイドラインが必要か？**
  - 社会的背景
  - 建設現場にとっての情報セキュリティとは
- **ガイドライン作成の方針**
  - ガイドラインを作成する目的と想定する読者
- **ガイドラインの概要**
  - ガイドライン目次の紹介
  - ISMSとオフィスセキュリティマークをベースとしての検討
- **セキュリティ対策の進め方**
  - 基本的な流れ
- **ガイドライン発刊スケデュール**

１．何故セキュリティガイドラインが必要なのか？

■社会的背景

（１）　ＩＴの導入活用拡大にともなう情報
・セキュリティリスクの増大
・情報漏洩、機器盗難等の事故の多発

（２）　法的規制や各種ルールの強化
・個人情報保護法や内部統制強化への対応

（３）　ＩＳＭＳへの関心の高まり
・経営者主導によるトップダウンの取り組み
・機密性・完全性・可用性のバランス

機密性	アクセス権を持つ者だけがアクセスできる
完全性	情報および情報処理が完全である
可用性	必要な時に情報にアクセスできる

（４）　建設現場における情報管理の重要性
・ＪＶ各社の情報セキュリティ強化
・情報管理・情報共有・情報セキュリティの連携
・業界横断的なガイドラインの必要性

１．何故セキュリティガイドラインが必要なのか？

■建設現場にとっての情報セキュリティとは

（１）建設現場（事務所）でもリスクが増大している

●業務で取り扱う情報の電子化が進展

・顧客情報、予算、見積り・・
・建物情報、設計図面
・施工図、竣工図
・協力会社情報・・

→ 情報システム化
パソコン、ネットワーク利用の増加

●セキュリティ事故が増大

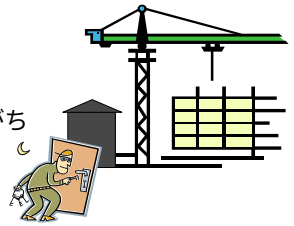
・パソコン、外部記憶媒体の盗難、紛失
・不正ソフト利用、ウィルス感染によるネットワークからの情報漏洩
・データの誤送信、操作ミスによる情報漏洩
・従業員、委託業者の不正データ持出しによる情報漏洩

１．何故セキュリティガイドラインが必要なのか？

■建設現場にとっての情報セキュリティとは

（２）建設現場（事務所）の特徴とセキュリティ面での注意ポイント

●建設現場の特徴と注意ポイント



①仮設事務所が多い
→侵入しやすく、空巣に狙われる
→オフィスビルよりも警備が手薄になりがち

②外部から多数の人の出入りが多い
→機密書類やパソコン画面の盗み見
→書類や記録媒体の盗難

③ＪＶなどで複数企業体で運営されることが多い
→各社のセキュリティレベルがアンマッチ
→弱いところから情報漏洩が発生する

④必要な情報は共有しないと仕事にならない
→管理面があいまいになりがち

１．何故セキュリティガイドラインが必要なのか？

■建設現場にとっての情報セキュリティとは

（３）建設現場の情報セキュリティ対策

●建設現場の特徴(注意ポイント)を考慮した以下の対策を実施し、セキュリティリスクを低減

管理面での対策

①組織
・セキュリティ方針、体制
・事故時の報告、再発防止

②物理的
・機械警備等の侵入対策
・機器の盗難防止
・入退出管理

③人的
・誓約書締結、罰則規定
・機密保持契約締結
・セキュリティ教育

IT面での対策

①情報漏洩防止
・データの暗号化
・アクセス制限
・アクセス権限管理
・ログ取得

②ウィルス対策

③データバックアップ

④情報ｼｽﾃﾑ、ｲﾝﾀｰﾈｯﾄ、機器等の利用ルール

２．ガイドライン作成の方針

■ガイドラインを作成する目的と想定する読者層

作成の背景：

☐ 建設現場にも情報セキュリティ対策が必要な時代になってきた

☐ 作業所向けの情報セキュリティ基準がない

作成に当たって考慮したこと：

☐ 個々の作業所にあった適用ができるように、情報セキュリティの考え方を提示

☐ 実際に使えるように、具体的な事例を挙げて作成

☐ すぐに利用できる規定類の雛形を提示

ガイドラインの読者層：

☐ 情報セキュリティは、作業所員全員が取り組まなければならない問題

☐ 作業所長が中心となって、所員全員が対象

２．ガイドライン作成の方針

■ISMSとオフィスセキュリティマークをベースとしての検討

☆セキュリティーに関する認証制度

- **プライバシマーク（財）日本情報処理開発協会（JIPDEC）**
  - プライバシーマーク制度は、事業者が個人情報の取扱いを適切に行う体制等を整備していることを認定し、その証として“プライバシマーク”の使用を認める制度
- **ＩＳＯ２７００１関連（JIPDEC･JSA･JAB･JQA）**
  - 情報セキュリティ マネジメントシステムに関する国際標準規格（ISO）です。
  - 審査登録機関が、ISMSの認証審査を実施する際の、基準となる**規格要求事項**が記載されています。
  - ISO9001（品質）や、ISO14001（環境）と同じく、PDCAモデルを採用しており、この規格要求事項を、組織の仕組みに導入することで、**組織の情報に関する取扱い**について、**継続的な改善**が期待できます。
- **オフィスセキュリティマーク**
  - オフィスにおける**物理的なセキュリティ対策**に関して、協議会が定めるオフィスセキュリティマーク認証基準に基づき、その基準を満たしている組織にマークの認証付与をおこなう制度です

２．ガイドライン作成の方針

■ISMSとオフィスセキュリティマークをベースとしての検討

昭和56年7月

情報システム安全対策実施事業所認定制度

・施設・設備の物理的セキュリティが中心

【問題点】

・人的セキュリティ対策を加えた全社統合的なマネジメントの必要性

平成14年4月

ISMS適合性評価制度

・「人」「物」「金」「情報」の経営資源を**総合的に管理**

・大組織向き

平成18年10月

オフィスセキュリティマーク認証制度

・「物」「金」を対象に**具体的化**

・**小組織向き**

【対象は】

現場事務所
工事現場

【対策は】

ISMS
の全社統合的なマネジメントの考え方を軸に、
オフィスセキュリティマーク
の具体的対策を現場事務所に利用

３．ガイドラインの概要

■ガイドラインの目次

	はじめに	作成の目的 想定する読者等 他のガイドラインとの位置づけ
1	建設現場情報セキュリティ強化の背景	社会的背景 建設現場の情報ｾｷｭﾘﾃｨとは
2	ISMSﾌﾚｰﾑﾜｰｸから見た建設現場の情報ｾｷｭﾘﾃｨ管理	ISMSとは ISMS要求事項と現場ｾｷｭﾘﾃｨとの関係 ｵﾌｨｽｾｷｭﾘﾃｨﾏｰｸと現場ｾｷｭﾘﾃｨ管理
3	建設現場の情報ｾｷｭﾘﾃｨ管理体制の構築と運用手順	構築の手順 運用方法 対策の見直し

３．ガイドラインの概要

■ガイドラインの目次

4	建設現場で実施すべき対策と対策例	基本方針と組織 情報資産の管理 人的資源のｾｷｭﾘﾃｨ 物理的環境的資源のｾｷｭﾘﾃｨ 通信環境及びアクセス制御のｾｷｭﾘﾃｨ
5	ＪＶ各社が実施すべき対策と対策例	ＪＶ各社のｾｷｭﾘﾃｨﾎﾟﾘｼの違いについて 各社専用の通信と運用管理 各社独時のアクセス管理 各社独自のシステム運用 管理部門との協調
	終わりに	

３．ガイドラインの概要

■ISMSとオフィスセキュリティマークをベースとしての検討

☆オフィスセキュリティマークの認証基準

・事務所内エリアのセキュリティレベル定義

レベル１	入室の抑制機能があり、且つ無断入室禁止等の表示があること
レベル２	アクセス制限が規定され常時施錠の居室、またはレベル１エリア内にある常時施錠され、アクセスが規定された保管庫・キャビネット等
レベル３	アクセス権限が規定され、且つアクセス記録が取られている居室、またはレベル１エリア以上の仲にある常に施錠され、アクセス権限が規定され、アクセス記録が取られている保管庫・キャビネット等

３．ガイドラインの概要

■ISMSとオフィスセキュリティマークをベースとしての検討

☆オフィスセキュリティマークの認証基準

・保護対象資産の分類と保護対策

重要度１	レベル１エリアに保管・保存	漏洩または損失等が生じた場合、業務への影響が比較的少ない有形の経営資産
重要度２	レベル２エリアに保管・保存	漏洩または損失等が生じた場合、業務に大きな影響を与える可能性のある有形の経営資産
重要度３	レベル３エリアに保管・保存	漏洩または損失等が生じた場合、事業の継続に大きな影響を与える可能性のある有形の経営資産

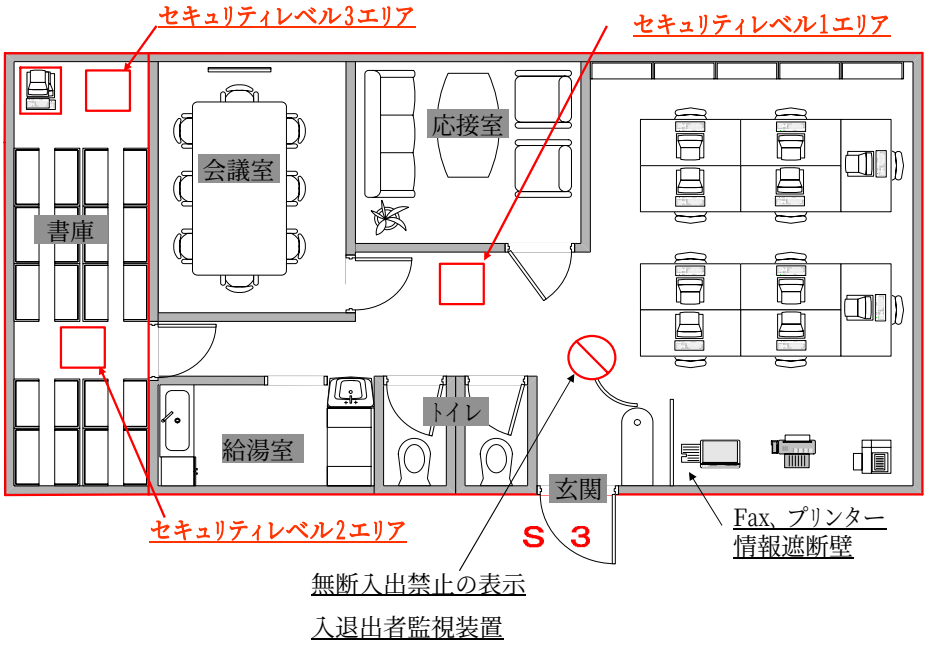
３．ガイドラインの概要

■ISMSとオフィスセキュリティマークをベースとしての検討

☆オフィスセキュリティマークの認証基準（その他の基準）

書類等の廃棄及び再利用	・１年を超えて保存する必要がある書類等については保存期間が定められていること。 ・書類又はデジタル媒体等の廃棄について適切な対策が取られている事 ・重要度２以上の資産は再利用しない
配送物管理	・配送物に関しては盗難対策が取られている事
情報通信機器等の管理	・コピー機、FAX又はプリンタ等書類の出力等を行う装置及び出力物については、機密保護対策が取られている事 ・ノートブックパソコンは業務終了後には盗難防止対策が取られている事 ・ノーブックパソコンは管理責任者の許可無しにエリア外に持ち出すことが禁止されていること
従業員等の識別管理及び鍵等の管理	・従業員等の識別管理が適正に行われていること ・居室又は保管庫等の鍵は適切に管理され、紛失時は適切な対策がとられていること

■ 現場事務所のセキュリティ管理イメージ



4．セキュリティ対策の進め方

【基本的な流れ】

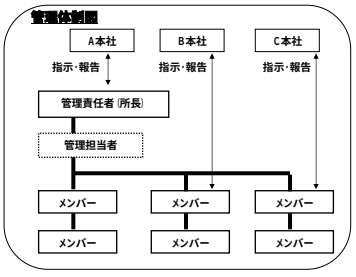
Ⅰ．現場所長がセキュリティ対策を策定・周知（P）します。

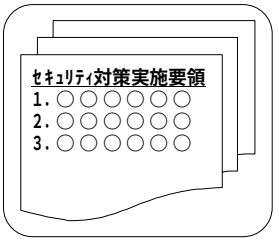
Ⅱ．策定した対策を実行（D）・点検（C）します。

Ⅲ．必要に応じて見直し（A）ます。

【Ⅰ：策定・周知】

- **体制の確立 ⇒ 「管理体制図」**
- **範囲（資産）の洗い出し ⇒ 「情報資産一覧表」**
- **リスク評価をし実施策を決定 ⇒ 「セキュリティ対策実施要領」**





４．セキュリティ対策の進め方

【Ⅱ：実行・点検】

「セキュリティ対策実施要領」を実行します。


ルールの遵守、作業の記録、定期的な確認

（具体的には、、

整理整頓、無人時の施錠、台帳の更新、定例会議での確認、、、、

【Ⅲ：見直し】

必要に応じて、対策を見直します。

⇒【Ⅰ：策定・周知】⇒【Ⅱ：実行・点検】⇒【Ⅲ：見直し】⇒　⇒　⇒

「見直しが必要な原因とは、」

職場の環境変化

（人員や情報資産の大幅な増減等）

本社からの指示

セキュリティ事故や不具合の発生　　等々

■ガイドライン発刊までの予定

○６月～10月：執筆

（BCS＆土工協会員会社ｾｷｭﾘﾃｨ担当者による）

○10月～12月：校正

○平成20年4月：初版発刊

○平成20年4月～

・利用者意見聴取

・第2版　検討

建設現場の
情報セキュリティガイドライン

問い合わせ・連絡先

(社）建築業協会 IT推進部会 cals_bcs@bcs.or.jp

情報基盤セキュリティ専門部会

北沢 孝宗	鹿島建設
高馬 洋一	間組
児山 満	前田建設工業
柴田 耕作	三菱マテリアル
豆腐谷 洋一	竹中工務店
友枝 幸一	戸田建設
長谷 芳春	三井住友建設