情報セキュリティリスクの軽減に向けて

～サイバーセキュリティ月間～
（2/1～3/18）

2019.3.1　建築のITセミナー
情報セキュリティ専門部会

NISC　内閣サイバーセキュリティセンター

NISC　HPより

サイバー空間での
国民生活や社会経済活動

サイバー犯罪の
被害者から加害者へ

東京オリンピック・パラリンピック

産・学・官・民が連携して

首相官邸のHPより

『約束のネバーランド』とタイアップ

©白井カイウ・出水ぽすか／集英社・約束のネバーランド製作委員会

NISC　HPより

2019.01.23
「サイバーセキュリティ月間」に伴う情報セキュリティの強化」を発信しました。

サイバー月間　セキュリティポスター

【その投稿、ちょっと待った！】

（建設現場内、および事務所内掲示用）

サイバー月間　パンフレット

【情報漏えい防止徹底について】

（建設現場内掲示用）

協力会社向け
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について～
情報管理も大事な仕事の一つです

（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）
- 当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、「情報」が漏れてしまったら・・・>>>
万が一「情報」が漏えいしたら、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ます。
（例え過失でも、解雇や懲戒などの可能性もあります）
- 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もいなかった・・・。

- 私物（自宅）パソコンで仕事をしていた。見慣れない発信者からのメールの添付ファイルを開いたら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メールがすべて流出した。
- パソコンを電車に置き忘れたら、ネットオークションで販売されてデータも流出した。
- 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訴え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。
  - 公衆の場（公共交通機関・飲食店、等）では仕事の話をしないようにしましょう。
- 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SNS、ブログ（個人日記）、掲示板、プライベートのメールなどに書き込む。
  - 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　しっかりと保管する >>>

- 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。パソコンをセキュリティワイヤーで固定するなど、物理的な防犯対策も大切です。

ポイント7「情報」の持ち出しや持ち歩きには注意する >>>

- 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やスマートデバイスには、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なってください。
- 職場の外では肌身離さないよう注意してください。電車移動の際、網棚や座席、座席ポケットに置いたり、駐車時に車中に放置してはいけません。
- 持ち出し時には、目的地に直行してください。
  - 外食や飲酒、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「情報」の社外への送信は最小限にとどめ、誤配に注意する >>>

- 関係者に渡す「情報」は最小限にとどめてください。
- 郵送、FAX、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、必ず暗号化を行うか、パスワードを設定してください。
- 大容量のデータの送信にファイル転送サービスやオンラインストレージを使う場合は、会社が認める安全なサービスを利用してください。

ポイント9「情報」は確実に返却・廃棄する >>>

- 工事が完了したら、保管が認められた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細断するなど、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、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。

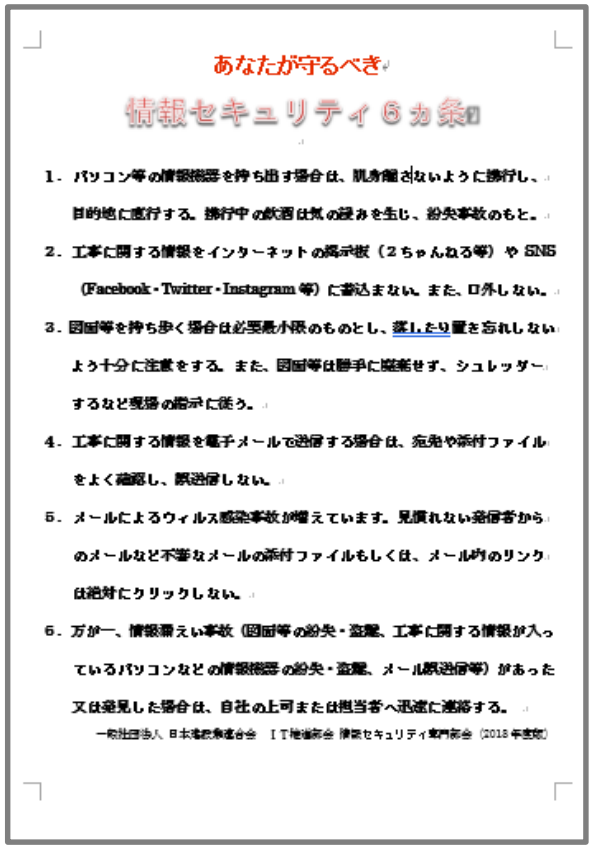
情報漏えい防止対策について、この資料に書かれていることで分からないことがありましたら、当社社員にお尋ねください。

一般社団法人 日本建設業連合会 IT推進部会 情報セキュリティ専門部会（2015 年度版）

サイバー月間　リーフレット

【あなたが守るべき　情報セキュリティ6カ条】

（建設現場内掲示、作業員受け入れ教育 配布用）



あなたが守るべき

情報セキュリティ６カ条

1．パソコン等の情報機器を持ち出す場合は、肌身離さないように携行し、目的地に直行する。携行中の飲酒は気の緩みを生じ、紛失事故のもと。

2．工事に関する情報をインターネットの掲示板（２ちゃんねる等）や SNS（Facebook・Twitter・Instagram 等）に書込まない。また、口外しない。

3．図面等を持ち歩く場合は必要最小限のものとし、落したり置き忘れしないよう十分に注意をする。また、図面等は勝手に廃棄せず、シュレッダーするなど現場の指示に従う。

4．工事に関する情報を電子メールで送信する場合は、宛先や添付ファイルをよく確認し、誤送信しない。

5．メールによるウィルス感染事故が増えています。見慣れない発信者からのメールなど不審なメールの添付ファイルもしくは、メール内のリンクは絶対にクリックしない。

6．万が一、情報漏えい事故（図面等の紛失・盗難、工事に関する情報が入っているパソコンなどの情報機器の紛失・盗難、メール誤送信等）があった又は発見した場合は、自社の上司または担当者へ迅速に連絡する。

一般社団法人 日本建設業連合会　ＩＴ推進部会 情報セキュリティ専門部会（2018 年度版）

1、情報機器の持ち出し

2、インターネットへの書き込み禁止

3、図面の取り扱い

4、電子メールの誤送信

5、不審メールへの注意

6、情報漏えい事故の報告

サイバー月間 （建築ーIT WEB）

建築 - IT WEB

- ＩＴ推進部会の紹介
- 建築ＩＴセミナー
- 情報セキュリティ
  - ガイドライン・教育資料集（協力会社向け含む）
- 先端ICT活用
- ＢＩＭ
- 成果集
- 関連　業界動向・リンク集・その他調査

「サイバーセキュリティ月間」に伴う情報セキュリティの強化

2019/01 発行

平成26年11月
ーセキュリティ
月1日から3月1
携による集中的
また、当会のI
情報セキュリテ
ガイドライン等
及促進を図って
建設作業員への
基本的事項を総
キュリティ月間
教育・啓発資料

本資料

資料

（1）「情報セキュリティポスター」

情報セキュリティポスター

（2）「情報セキュリティポスター」（英語版）

情報セキュリティポスター（英語版）

（3）「情報漏えい防止徹底パンフレット」

情報漏えい防止徹底パンフレット

（4）「情報セキュリティ6か条リーフレット」

情報セキュリティ6か条リーフレット

Society 5.0

スマートシティ

i-Construction

建設キャリアアップシステム

ＡＩ　ＩｏＴ

BIM　CIM

クラウドサービス

サイバー攻撃

働き方改革

情報漏えい

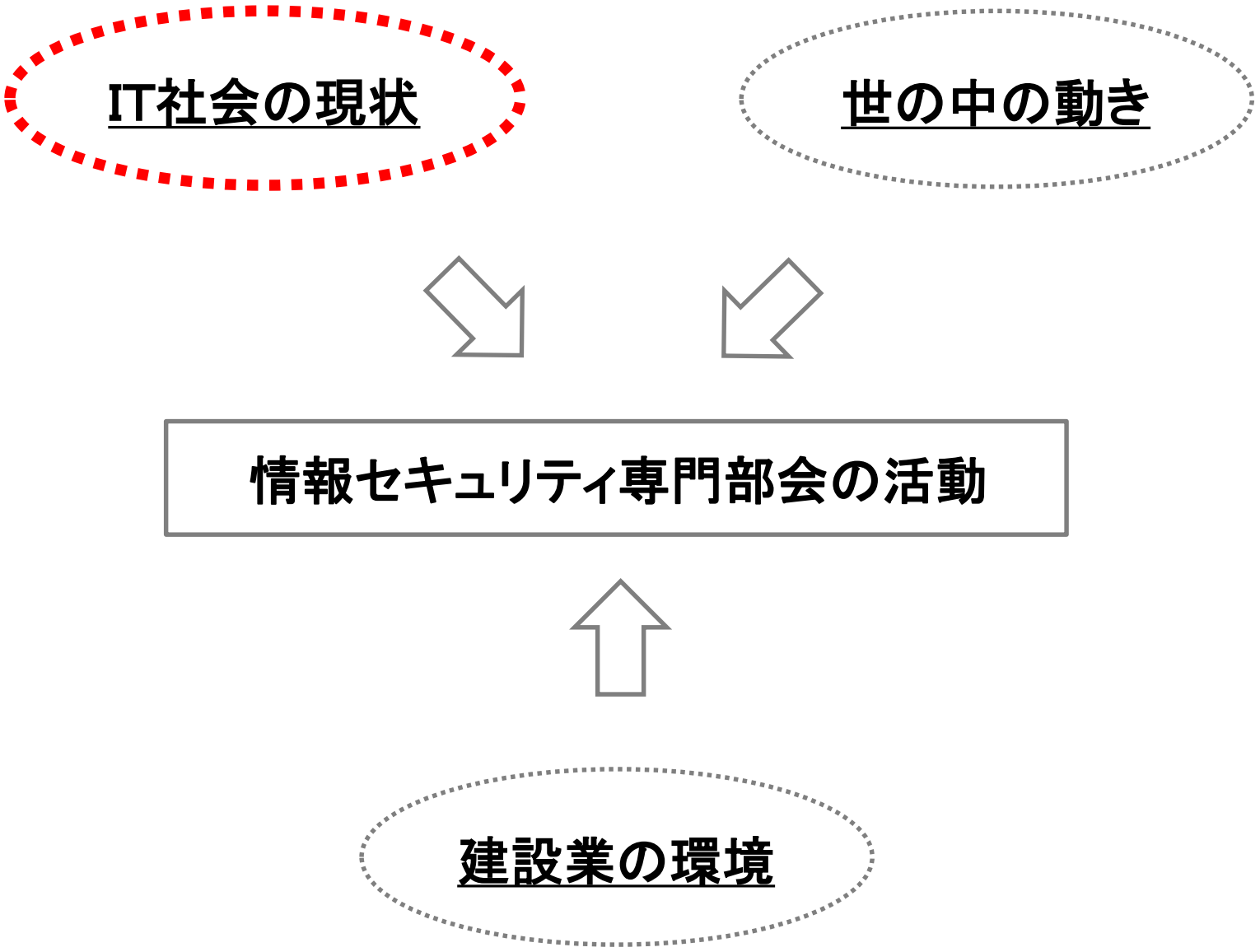
サイバー月間 （内閣府）

５G

仮想通貨流出

個人情報保護

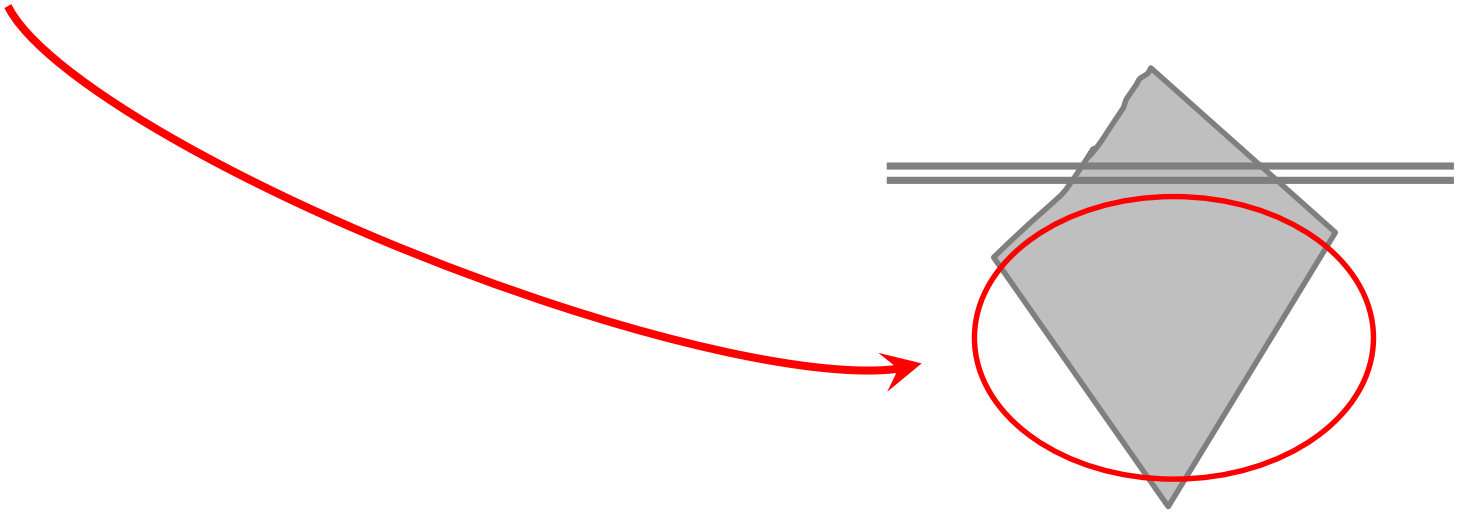
経済産業省【サイバーセキュリティ経営ガイドライン】



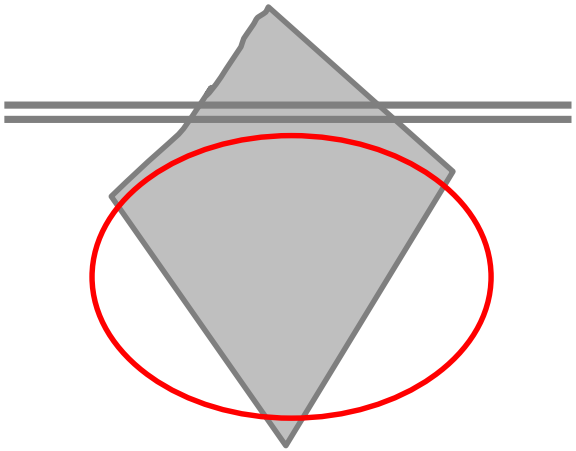
【現在のサイバー犯罪とは】

- ✔ 組織化・分業化
- ✔ 全自動化
- ✔ 見えない
- ✔ 闇市場（ダークweb、Under Ground）

☛ 増え続けている



✔ 闇市場（（ダークweb、Under Ground））



あなたのPWD、漏れてませんか？

増え続けている「サイバー犯罪」 ☛ 対策は？

- ✔ リスクの可視化
- ✔ 体制整備
- ✔ 教育・訓練

建設業が参考とされている！

体制図・KY活動・入場者教育・・・

2017年個人情報漏えい事故（JNSA：日本ネットワークセキュリティ協会）

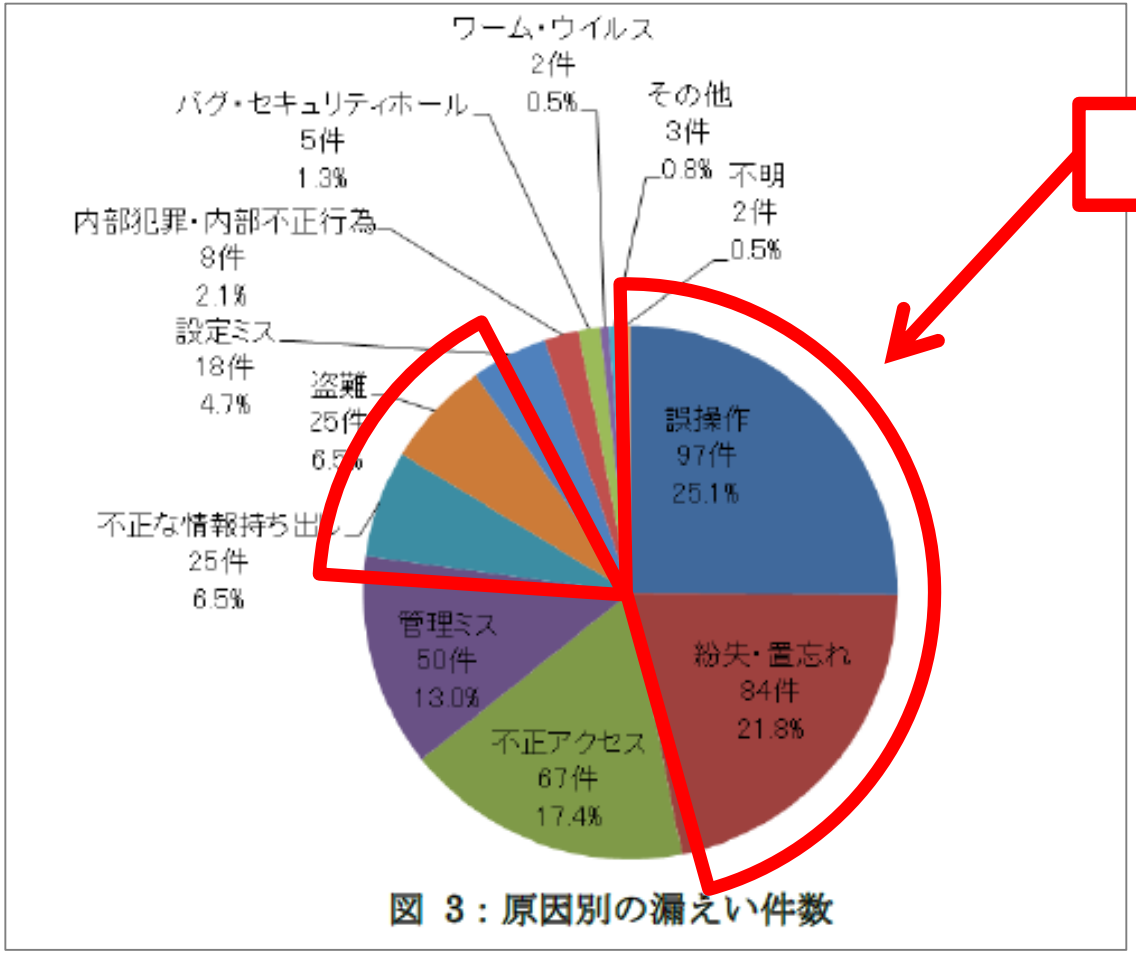


図 3：原因別の漏えい件数

利用者が原因　約60%

誤操作	25.1%
紛失・置忘れ	21.8%
不正な持ち出し	6.5%
盗難	6.5%

IT社会の現状

ーポイントー

- ✔ 増え続けるサイバー攻撃
- ✔ 利用者を起因とする情報漏えい事故が多い

IT社会の現状

- ✔ 増え続けるサイバー攻撃
- ✔ 利用者を起因とする情報漏えい事故が多い

世の中の動き

情報セキュリティ専門部会の活動

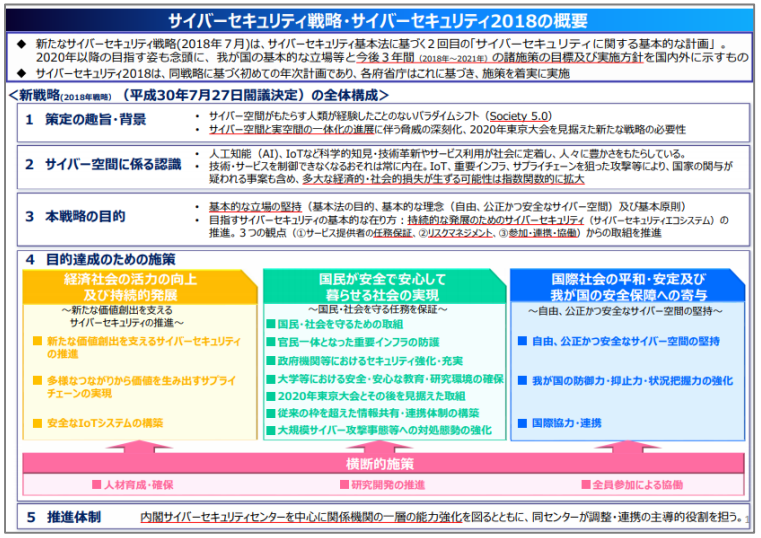
建設業の環境

「サイバーセキュリティ2018」

2018 年7月 25 日サイバーセキュリティ戦略本部

本書は、我が国のサイバーセキュリティ政策に関する国家戦略であり、

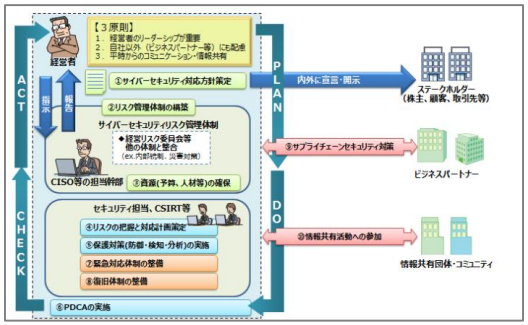
1. 経済社会の活力の向上及び持続的発展
2. 国民が安全で安心して暮らせる社会の実現
3. 国際社会の平和・安定及び我が国の安全保障への寄与
4. 横断的施策
5. 推進体制



【サイバーセキュリティ経営ガイドライン】

✔ 経済産業省　2017年11月16日

経営者に対しての
　3原則　と　10の指示事項



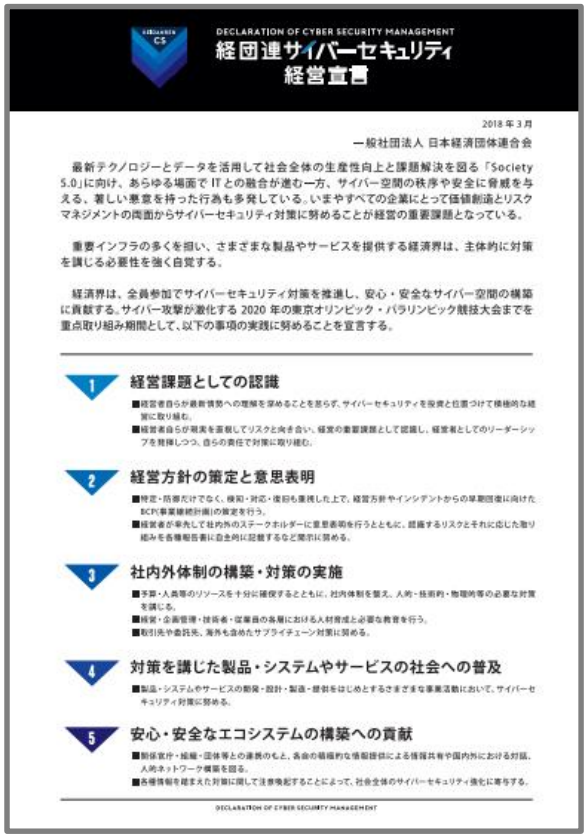
✔　経営者のリーダーシップが重要

✔　自社以外（ビジネスパートナー等）にも配慮

✔　平時からのコミュニケーション・情報共有

【経団連サイバーセキュリティ経営宣言】

✔ 経団連　2018年3月



DECLARATION OF CYBER SECURITY MANAGEMENT

経団連サイバーセキュリティ
経営宣言

2018年3月

一般社団法人 日本経済団体連合会

最新テクノロジーとデータを活用して社会全体の生産性向上と課題解決を図る「Society 5.0」に向け、あらゆる場面でITとの融合が進む一方、サイバー空間の秩序や安全に脅威を与える、著しい悪意を持った行為も多発している。いまやすべての企業にとって価値創造とリスクマネジメントの両面からサイバーセキュリティ対策に努めることが経営の重要課題となっている。

重要インフラの多くを担い、さまざまな製品やサービスを提供する経済界は、主体的に対策を講じる必要性を強く自覚する。

経済界は、会員参加でサイバーセキュリティ対策を推進し、安心・安全なサイバー空間の構築に貢献する。サイバー攻撃が激化する2020年の東京オリンピック・パラリンピック競技大会までを重点取り組み期間として、以下の事項の実践に努めることを宣言する。

1 経営課題としての認識

■経営者自らが最新情勢への理解を深めることを基らず、サイバーセキュリティを投資と位置づけて積極的な経営に取り組む。
■経営者自らが現実を直視してリスクと向き合い、経営の重要課題として認識し、経営者としてのリーダーシップを発揮しつつ、自らの責任で対策に取り組む。

2 経営方針の策定と意思表明

■特定・防御だけでなく、検知・対応・復旧も重視した上で、経営方針やインシデントからの早期回復に向けたBCP(事業継続計画)の策定を行う。
■経営者が率先して社内外のステークホルダーに意思表明を行うとともに、認識するリスクとそれに応じた取り組みを各種報告書に自主的に記載するなど開示に努める。

3 社内外体制の構築・対策の実施

■予算・人員等のリソースを十分に確保するとともに、社内体制を整え、人的・技術的・物理的等の必要な対策を講じる。
■経営・企画管理・技術者・従業員の各層における人材育成と必要な教育を行う。
■取引先や委託先、海外も含めたサプライチェーン対策に努める。

4 対策を講じた製品・システムやサービスの社会への普及

■製品・システムやサービスの開発・設計・製造・提供をはじめとするさまざまな事業活動において、サイバーセキュリティ対策に努める。

5 安心・安全なエコシステムの構築への貢献

■関係官庁・組織・団体等との連携のもと、各自の積極的な情報提供による情報共有や国内外における対話、人的ネットワーク構築を図る。
■各種情報を踏まえた対策に関して注意喚起することによって、社会全体のサイバーセキュリティ強化に寄与する。

DECLARATION OF CYBER SECURITY MANAGEMENT

1. 経営課題としての認識

2. 経営方針の策定と意思表明

3. 社内外体制の構築・対策の実施

4. 対策を講じた製品・システムやサービスの社会への普及

5. 安心・安全なエコシステムの構築への貢献

世の中の動き

ーポイントー

- ✔ セキュリティ対策は経営の責務
- ✔ 協力会社と一体となった対応

IT社会の現状

✔増え続けるサイバー攻撃
✔利用者を起因とする
情報漏えい事故が多い

世の中の動き

✔セキュリティ対策は経営の責務
✔協力会社と一体となった対応

情報セキュリティ専門部会の活動

建設業の環境

建設業界の情報セキュリティ５大脅威　<2017年>

2017年に建設業界で影響の大きかったセキュリティ上の脅威を、日建連「情報セキュリティ専門部会」で実際に発生した事故をベースに選出し、順位付けした。
事故の原因は、本人の認識不足やルール違反と共に会社側の教育・指導不足があげられる。ひとたび事故が発生すると、施主の信用失墜や損害賠償などに繋がり、経営上の大きなリスクとなる。

順位	脅威	事例と解説
1	パソコン等の情報機器紛失・盗難	業務終了後、急遽酒席となり思わず泥酔してしまった。気が付くとパソコンが入った鞄ごと紛失していた。原則パソコンは持ち出さない。酒席となった場合は摂取量を控えるなど工夫ができるよう指導する。
2	ブログ等SNSへの投稿による現場写真の漏えい	現場作業員が現場の写真を個人のブログに投稿し、施主側が投稿に気づいた。スマホ世代(若者)に投稿傾向がみられる。新規入場者教育など業務の初期段階でしっかり意識付けすることが有効。
3	図面等重要書類の紛失・盗難による情報漏えいと事故報告遅延	図面紛失後、施主へ事故報告がなされないうちに、警察から施主に遺失物届連絡が入り、事故が発覚した。社員または協力会社への教育・指導力不足を疑われるので事故発生時の対応については繰返し確認することが必要。
4	メール誤送信による図面データ等の漏えい	メールの誤送信には宛先アドレスの間違いと添付ファイルの間違いの2パターンがある。いずれもメールを送る前に宛先アドレス、添付ファイルの中身をしっかり再確認することで回避可能。
5	標的型攻撃メールによるコンピュータウィルス(ランサムウェア＊1)感染	パソコンまたはサーバ上のファイルが暗号化され読取不可となり業務が停止。バックアップが無いと大きな手戻りが発生する。不審なメールの添付ファイルもしくはメール内のリンクは絶対にクリックしないよう指導すると共に疑似的攻撃メールを使った訓練も有効。

＊1　ランサムウェア　パソコンやサーバ内にあるファイルを暗号化し閲覧できない状態にしたりするウイルス。元の状態に戻すために仮想通貨などを支払うように求めてくる。日本をはじめ世界的に被害が広がっている。

建設業界の情報セキュリティ５大脅威　<2017年>

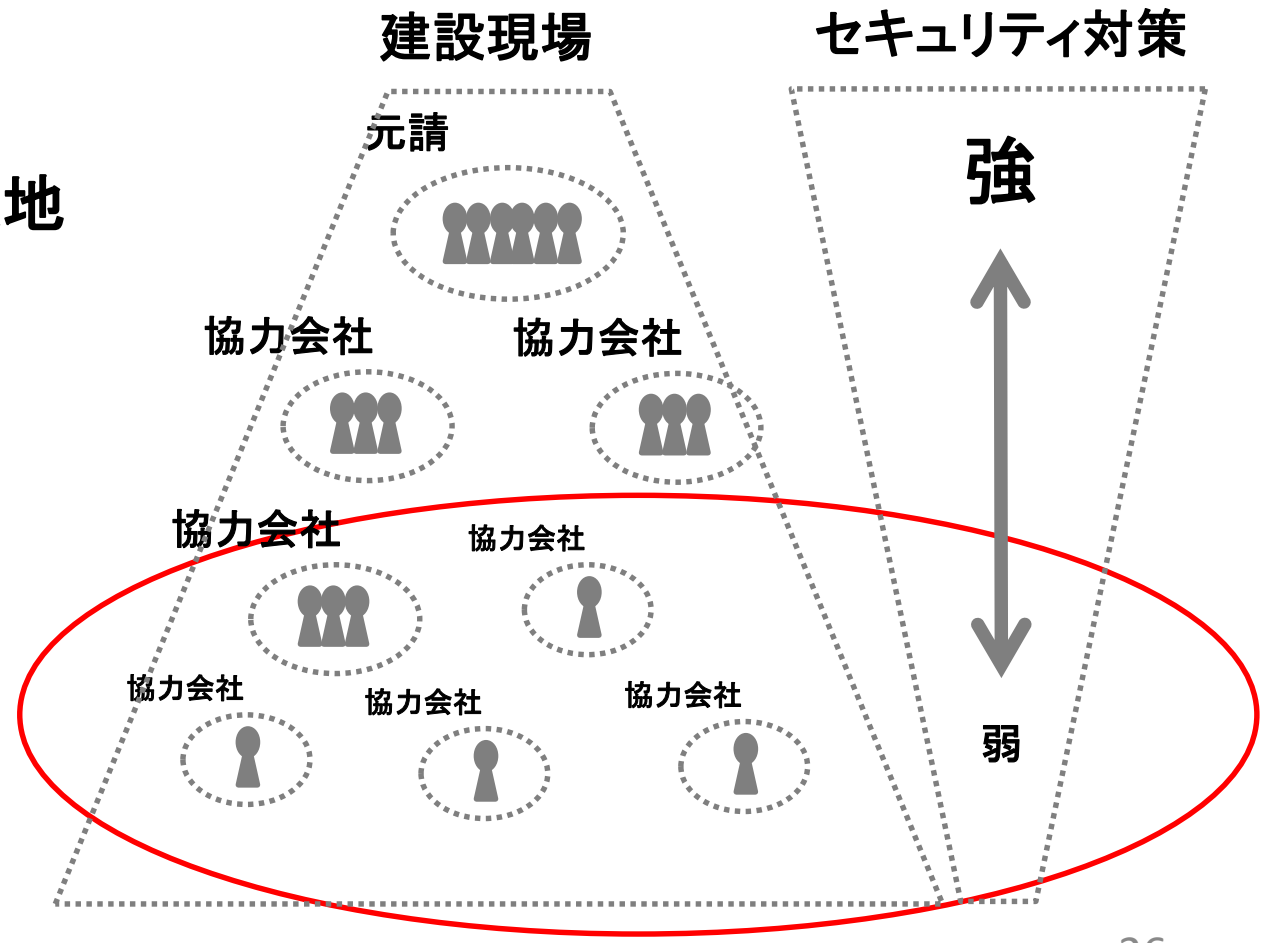
2017年に建設業界で影響の大きかったセキュリティ上の脅威を、日建連「情報セキュリティ専門部会」で実際に発生した事故をベースに選出し、順位付けした。
事故の原因は、本人の認識不足やルール違反と共に会社側の教育・指導不足があげられる。ひとたび事故が発生すると、施主の信用失墜や損害賠償などに繋がり、経営上の大きなリスクとなる。

順位	脅威	事例と解説
	パソコン等の情報機器紛失・盗難	業務終了後、急遽酒席となり思わず泥酔してしまった。気が付くとパソ

2017年に建設業界で影響の大きかったセキュリティ上の脅威を、日建連「情報セキュリティ専門部会」で実際に発生した事故をベースに選出し、順位付けした。
事故の原因は、本人の認識不足やルール違反と共に会社側の教育・指導不足があげられる。
ひとたび事故が発生すると、施主の信用失墜や損害賠償などに繋がり、経営上の大きなリスクとなる。

―「建設現場」特有の課題―

- ✔ 有期で出入りが多い
- ✔ 系列関係がない
- ✔ 職場が顧客の敷地



情報セキュリティ　桶の理論

工事情報＝桶の中の水

「一か所の不備（ex.協力会社）」から情報漏えい

ーポイントー

- ✔ 教育及び指導が重要
- ✔ 協力会社の底上げが必要

建設業の環境

IT社会の現状

✔増え続けるサイバー攻撃
✔利用者を起因とする
　情報漏えい事故が多い

世の中の動き

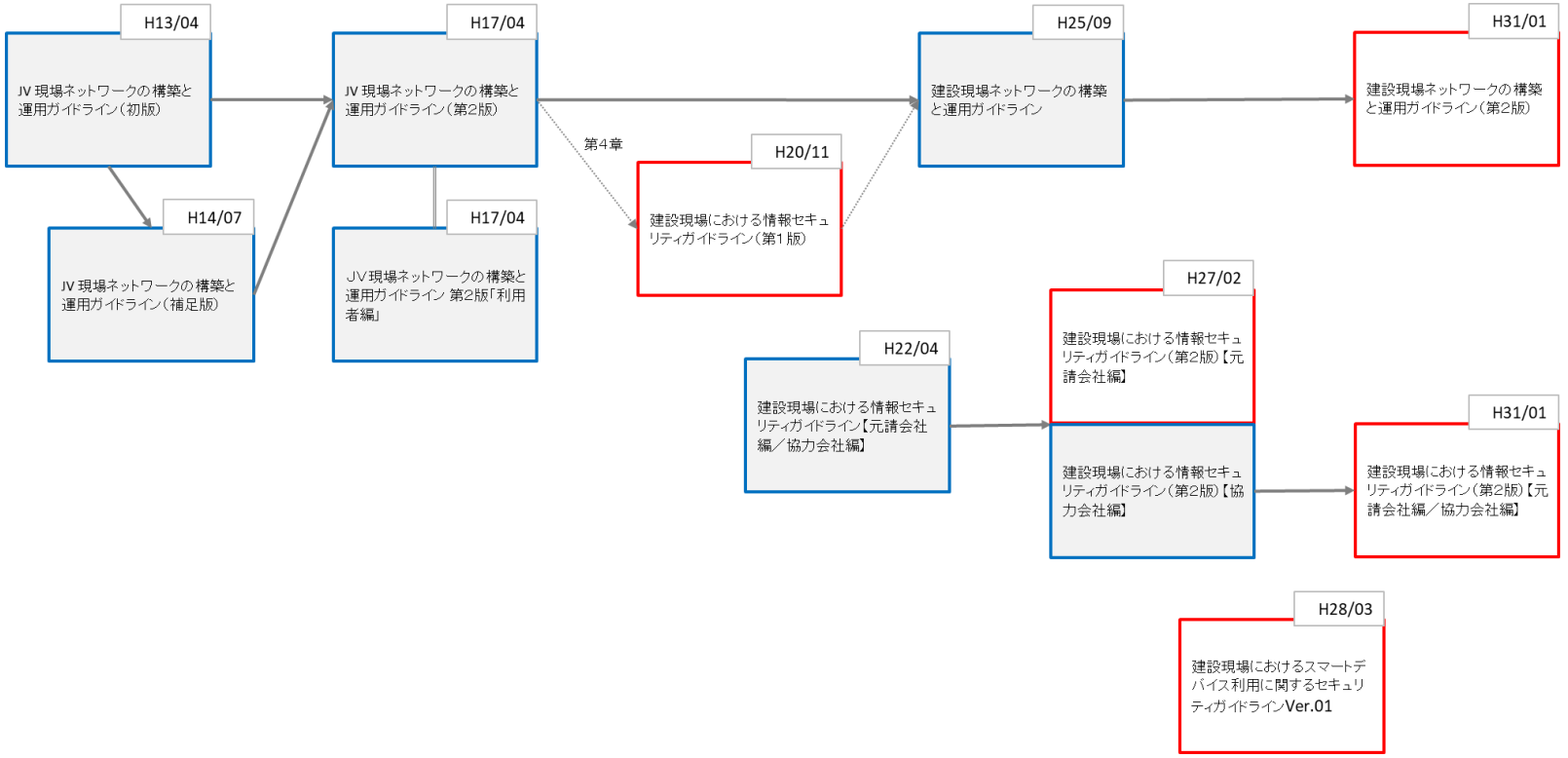
✔セキュリティ対策は経営の責務
✔協力会社と一体となった対応

情報セキュリティ専門部会の活動

建設業の環境

✔教育及び指導が重要
✔協力会社の底上げが必要

ガイドライン



これまで

2001年 「JV 現場ネットワークの構築と運用ガイドライン」から、のべ 12編 発行

改変を重ね、現在 5編 のガイドラインを公開

ガイドライン（公開）

Ⅰ	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）
	情報セキュリティマネジメントシステムの構築と運用手順、実施すべき事項を例示したもの
Ⅱ	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】
	“Ⅰ”を補完するもの。セキュリティ対策のなかでも重要な「情報漏えい」に焦点をあてたもの
Ⅲ	協力会社における情報セキュリティガイドライン
	協力会社が確実に実施すべき情報セキュリティ対策をとりまとめたもの
Ⅳ	建設現場ネットワークの構築と運用ガイドライン（第2版）
	建設現場のネットワーク構成とそこでのセキュリティの考え方、導入、維持管理方法について解説
Ⅴ	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
	誰でも手軽に利用できるスマートデバイスを活用するにあたっての基本的な考え方や注意点を解説

今年度　改定ガイドライン

協力会社における情報セキュリティガイドライン

目的　＝　改定のポイント

建設業が取り扱う情報は取引先の機密情報である

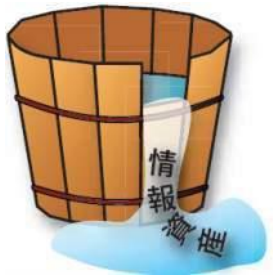
情報漏えいの多くは人的ミスが原因である

ルールの整備とその教育を通じた人的対策が有効

サイバー攻撃の脅威が高まっている

万全な対策をとることは不可能

確実に実施する対策を徹底することで最大の効果を上げる



協力会社における情報セキュリティガイドライン

会社としてやらなければならない４つの取り組み

（１）管理体制の構築

（２）実施する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の実施

（４）情報漏えいなどの事故発生時の対応

協力会社における情報セキュリティガイドライン

（一例）

（2）実施する情報セキュリティ施策とルール化

■技術面からの施策
・パスワードの管理
・ウィルス対策の実施、
①ウイルス対策ソフトの定義ファイルの最新化
②基本ソフト（OS）のセキュリティパッチの適用
業務で使うパソコンのOSやソフトウェアはメーカーサポートされているものを利用する。

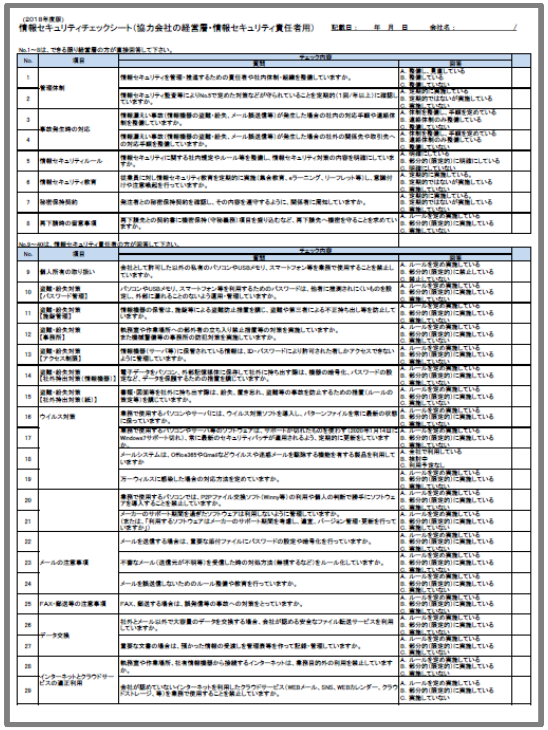
【注意】2019年12月末までにWindows 10に切替える。

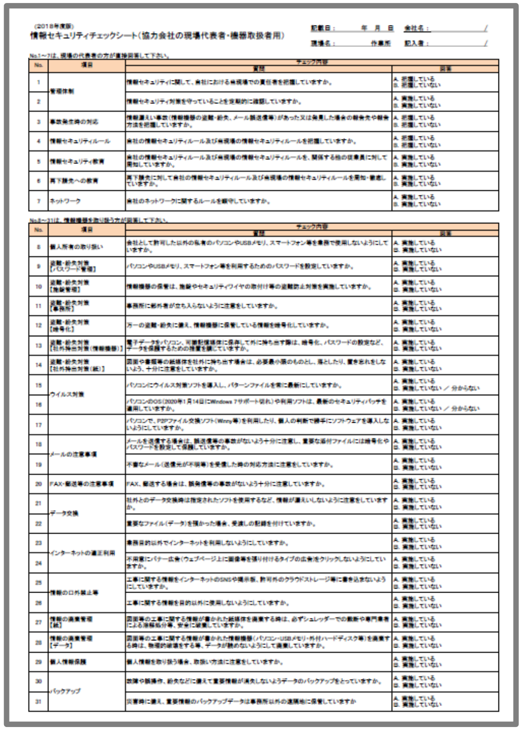
協力会社における情報セキュリティガイドライン

情報セキュリティチェックシート （建設業のひな型）

・協力会社の経営層・情報セキュリティ責任者用

・協力会社の現場代表者・機器取扱者用





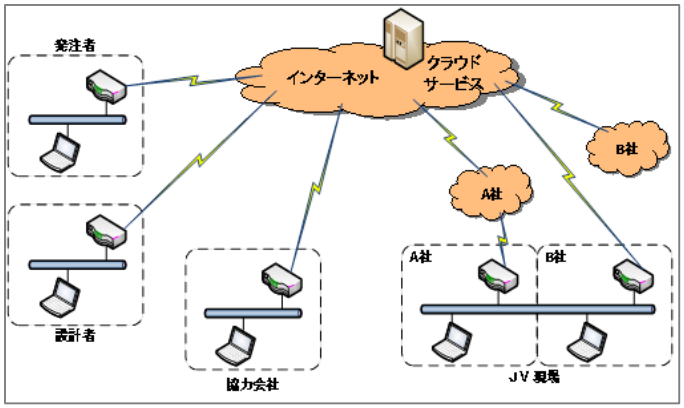
建設現場ネットワークの構築と運用ガイドライン（第2版）

目的　＝　改定のポイント

利用が拡大しているメッセンジャーやオンラインストレージといったクラウドサービスの利用に関する記述を中心に追加した

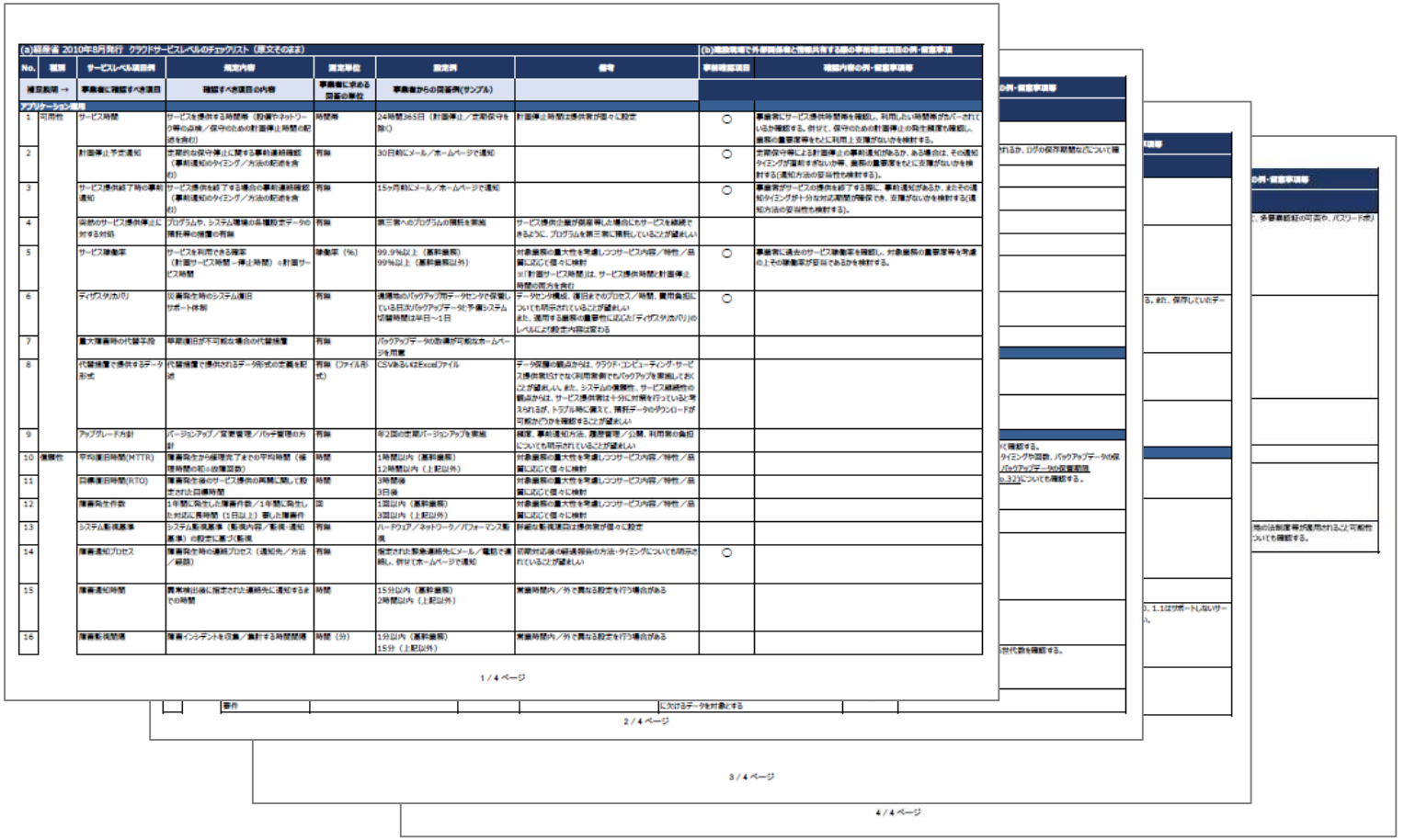
現状の情報セキュリティリスクに対応できる最低限の対策

個別のプロジェクト要件や新たに発生したセキュリティリスク等への対策については、関係者と協議・調整を十分に行ったうえで対応していただきたい



建設現場ネットワークの構築と運用ガイドライン（第2版）

クラウドサービスレベルのチェックリスト



日建連の取組

日建連：建築：建築−IT WEB

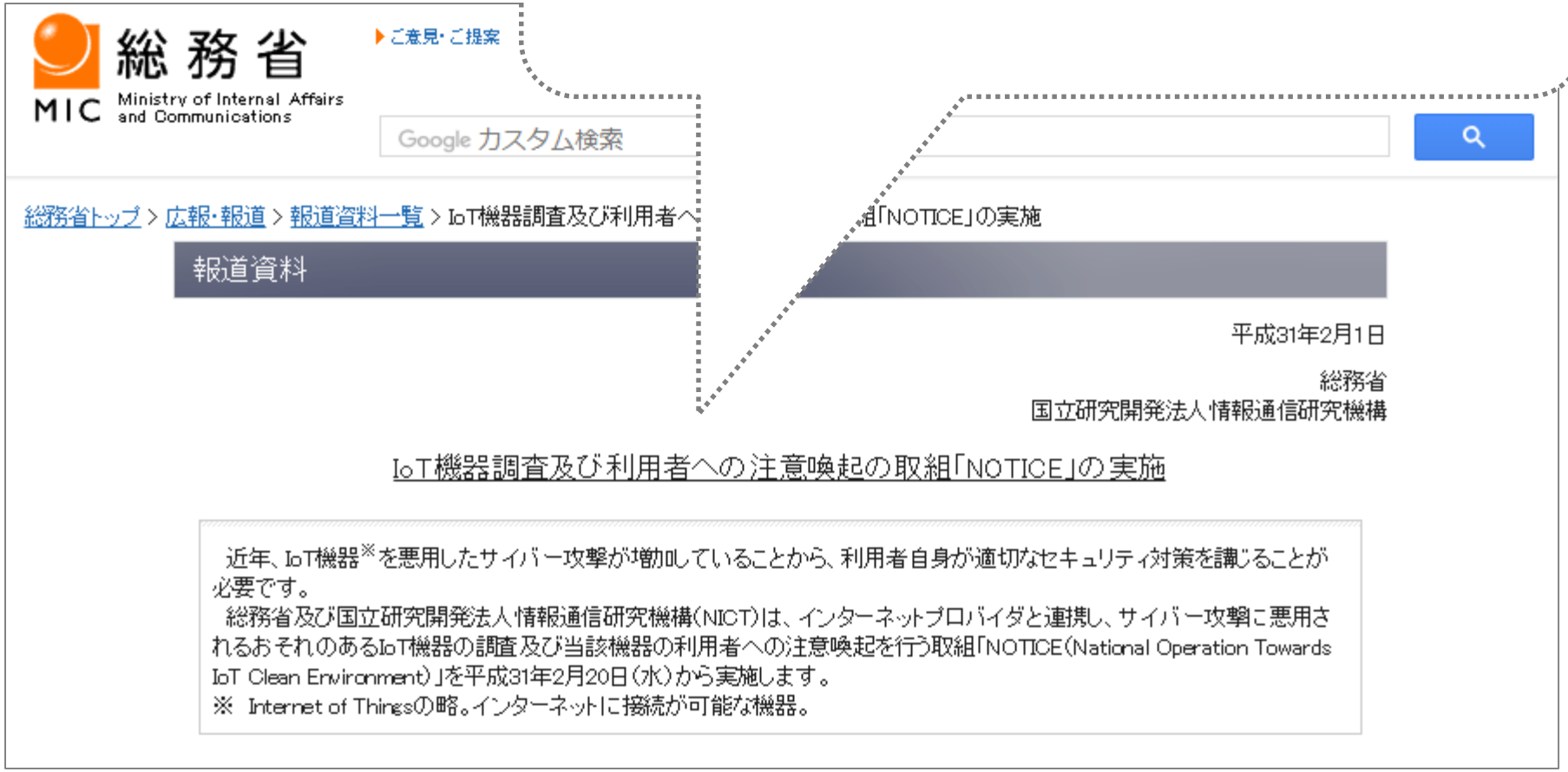
＞　ガイドライン・教育資料集
（協力会社向け含む）

事例紹介

NISC　HPより

事例紹介

IoT機器調査及び利用者への注意喚起の取組「NOTICE」の実施



総務省　MIC　Ministry of Internal Affairs and Communications

▶ご意見・ご提案

Google カスタム検索

総務省トップ > 広報・報道 > 報道資料一覧 > IoT機器調査及び利用者へ … 組「NOTICE」の実施

報道資料

平成31年2月1日

総務省
国立研究開発法人情報通信研究機構

IoT機器調査及び利用者への注意喚起の取組「NOTICE」の実施

近年、IoT機器※を悪用したサイバー攻撃が増加していることから、利用者自身が適切なセキュリティ対策を講じることが必要です。
総務省及び国立研究開発法人情報通信研究機構(NICT)は、インターネットプロバイダと連携し、サイバー攻撃に悪用されるおそれのあるIoT機器の調査及び当該機器の利用者への注意喚起を行う取組「NOTICE(National Operation Towards IoT Clean Environment)」を平成31年2月20日(水)から実施します。
※ Internet of Thingsの略。インターネットに接続が可能な機器。

総務省　HPより

事例紹介

平成31年2月20日（水）～

サイバー攻撃に悪用されるおそれのある機器を調査

当該機器の情報をインターネットプロバイダへ通知

インターネットプロバイダは、当該機器の利用者を特定し、注意喚起を実施

「NOTICE」ポスター

総務省　HPより

常に変化するリスク

前提：情報セキュリティ事故は発生する

「日々の対策」や「発生時の対応」
これを説明できることが重要

情報セキュリティ専門部会報告
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	安藤ハザマ	嶽野　聡	東急建設
相澤　健次郎	大林組	長沼　秀明	戸田建設
大塚　暁	鹿島建設	山口　正志	フジタ
小倉　弘至	清水建設	滝沢　強	前田建設工業
葛原　徹	大成建設	仙波　幹徳	三井住友建設
豆腐谷　洋一	竹中工務店		