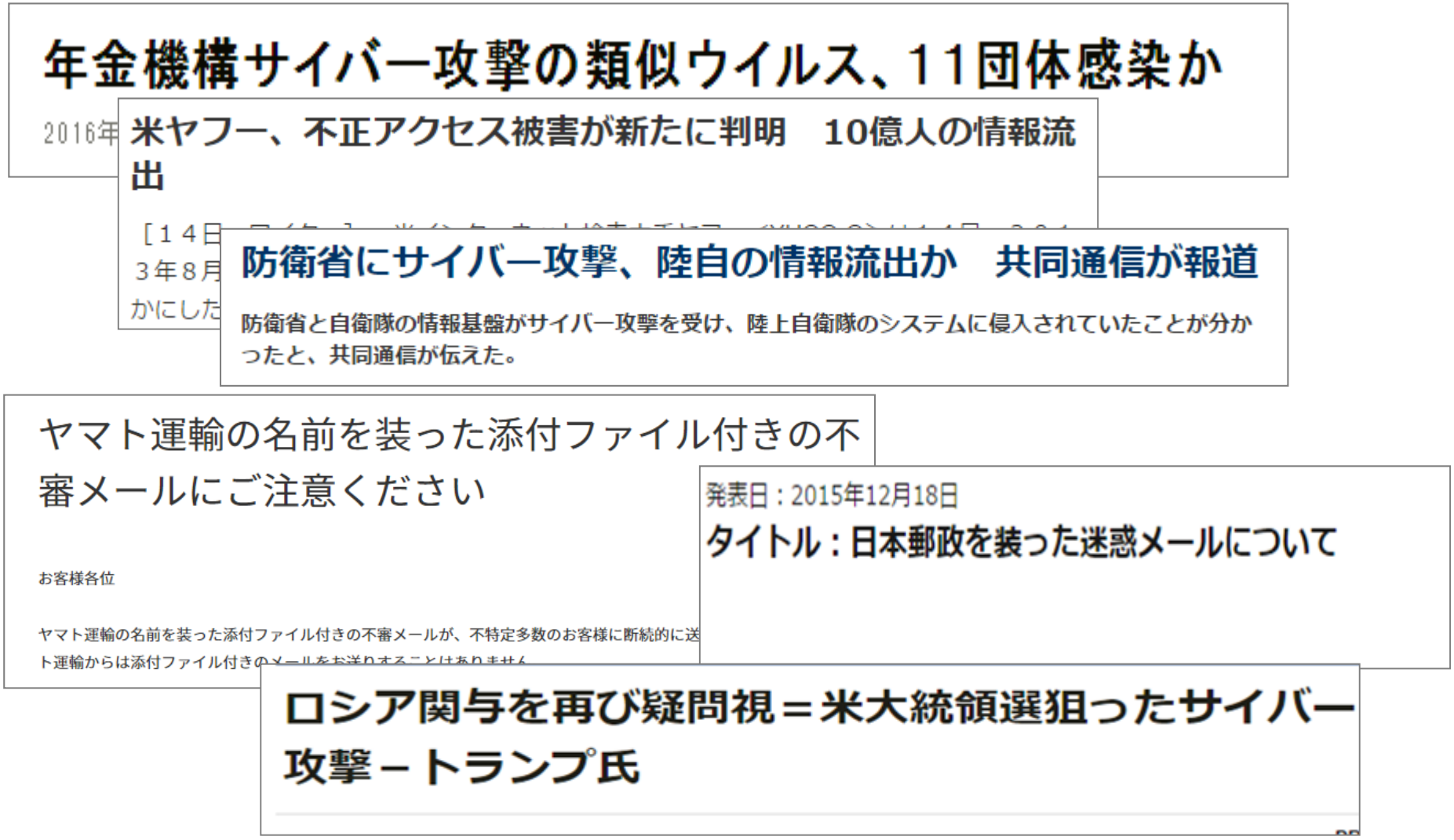
サイバー攻撃の実態と防御
～IoTの時代を迎えて～

2017/2/23「建築のITセミナー」

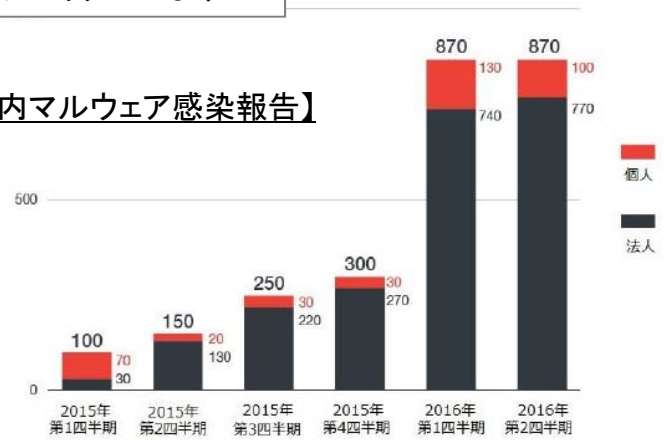
社会状況


年金機構サイバー攻撃の類似ウイルス、11団体感染か
2016年
米ヤフー、不正アクセス被害が新たに判明　10億人の情報流出
［１４日
３年８月
かにした
防衛省にサイバー攻撃、陸自の情報流出か　共同通信が報道
防衛省と自衛隊の情報基盤がサイバー攻撃を受け、陸上自衛隊のシステムに侵入されていたことが分かったと、共同通信が伝えた。
ヤマト運輸の名前を装った添付ファイル付きの不審メールにご注意ください
お客様各位
ヤマト運輸の名前を装った添付ファイル付きの不審メールが、不特定多数のお客様に断続的に送
ト運輸からは添付ファイル付きのメールをお送りすることはありません
発表日：2015年12月18日
タイトル：日本郵政を装った迷惑メールについて
ロシア関与を再び疑問視＝米大統領選狙ったサイバー攻撃－トランプ氏

社会状況

トレンドマイクロHPより

【国内マルウェア感染報告】

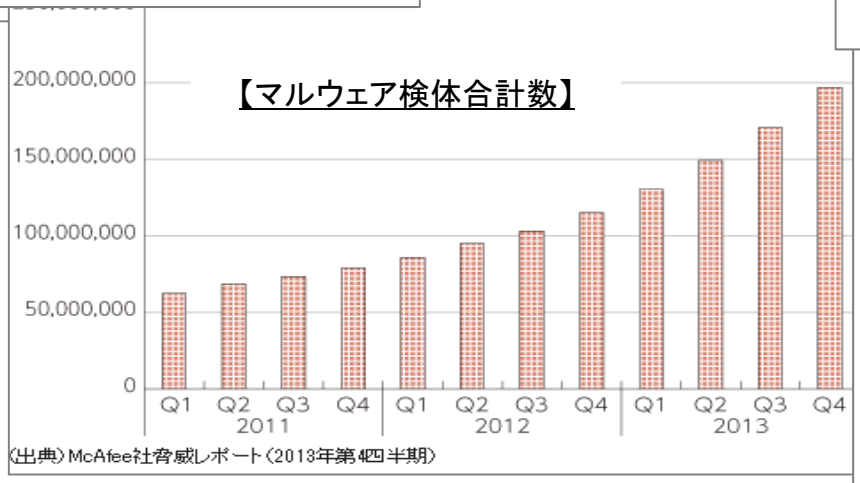


警察庁発表

【標的型メール報告件数】

総務省HPより

【マルウェア検体合計数】

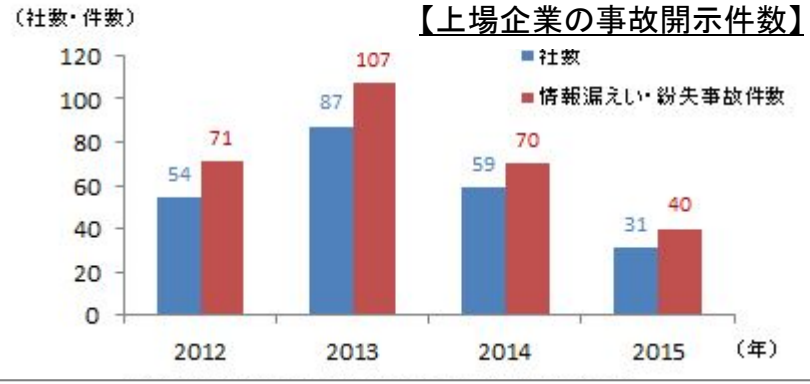


(出典)McAfee社脅威レポート(2013年第4四半期)

東京商工リサーチHPより

漏えい・紛失事故 年次推移

【上場企業の事故開示件数】



国の取組（基本法、内閣）

✔2014年11月 「サイバーセキュリティ基本法」

2015年1月

内閣に「サイバーセキュリティ戦略本部」

内閣官房に「内閣サイバーセキュリティセンター（NISC）」

国の取組（国土交通省）

2016年6月 「国土交通省IT政策検討会報告書」

目　　次

２．ITを巡る動向と今後の見通し

（keyword）

〇建設現場におけるIT･IoTについての取組
〇スマートシティに向けた取組

〇サイバー攻撃･･･東京オリンピック･･･
　　･･攻撃がさらに活発化･･

国の取組（国土交通省）

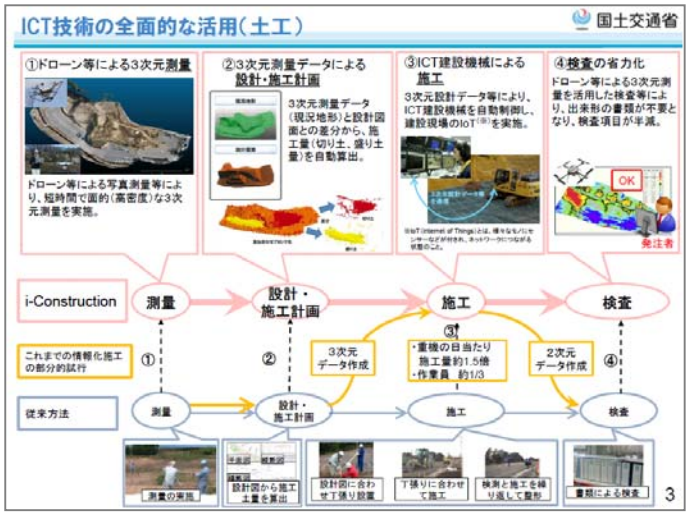
2016年6月 「国土交通省IT政策検討会報告書」

目　　次

3．ITの利活用に関する国土交通省における取組状況

（keyword）

〇「i-Construction」の取組を推進



国の取組（国土交通省）

2016年6月 「国土交通省IT政策検討会報告書」

目　　次

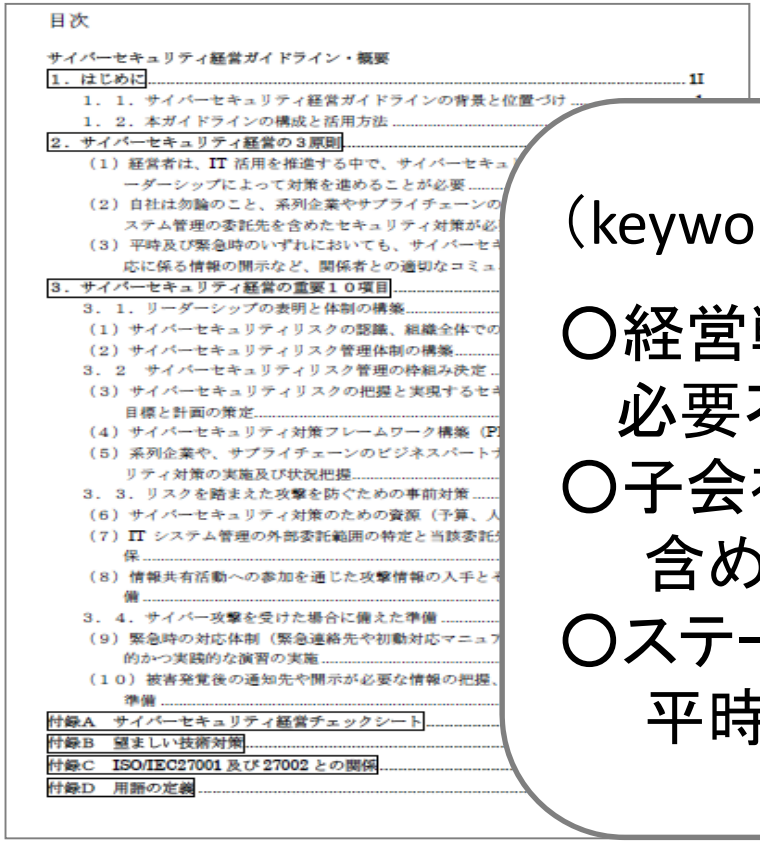
4. 今後の取組の方向性

（keyword）

- ○サイバーセキュリティ対策の推進
- ○情報共有体制の構築
- ○重要インフラにおける対策の徹底・深度化
  （鉄道・航空・物流）
- ○中小企業の底上げ対策の実施

国の取組（経済産業省）

2015年12月 「サイバーセキュリティ経営ガイドライン」
2016年12月 「サイバーセキュリティ経営ガイドライン」Ver1.1


目次

サイバーセキュリティ経営ガイドライン・概要
1．はじめに……1
1．1．サイバーセキュリティ経営ガイドラインの背景と位置づけ……
1．2．本ガイドラインの構成と活用方法……
2．サイバーセキュリティ経営の３原則
（1）経営者は、IT 活用を推進する中で、サイバーセキュ
ーダーシップによって対策を進めることが必要……
（2）自社は勿論のこと、系列企業やサプライチェーンの
ステム管理の委託先を含めたセキュリティ対策が必
（3）平時及び緊急時のいずれにおいても、サイバーセキ
応に係る情報の開示など、関係者との適切なコミュ
3．サイバーセキュリティ経営の重要１０項目
3．1．リーダーシップの表明と体制の構築……
（1）サイバーセキュリティリスクの認識、組織全体での
（2）サイバーセキュリティリスク管理体制の構築……
3．2 サイバーセキュリティリスク管理の枠組み決定
（3）サイバーセキュリティリスクの把握と実現するセキ
目標と計画の策定……
（4）サイバーセキュリティ対策フレームワーク構築（P
（5）系列企業や、サプライチェーンのビジネスパートナ
リティ対策の実施及び状況把握……
3．3．リスクを踏まえた攻撃を防ぐための事前対策……
（6）サイバーセキュリティ対策のための資源（予算、人
（7）IT システム管理の外部委託範囲の特定と当該委託
保……
（8）情報共有活動への参加を通じた攻撃情報の入手とそ
備……
3．4．サイバー攻撃を受けた場合に備えた準備……
（9）緊急時の対応体制（緊急連絡先や初動対応マニュア
的かつ実践的な演習の実施……
（10）被害発覚後の通知先や開示が必要な情報の把握、
準備……
付録A サイバーセキュリティ経営チェックシート……
付録B 望ましい技術対策……
付録C ISO/IEC27001 及び 27002 との関係……
付録D 用語の定義……

（keyword）

〇経営戦略としてのセキュリティ投資は
必要不可欠かつ経営者としての責務である
〇子会社・系列企業・サプライチェーンを
含めたセキュリティ対策が必要
〇ステークホルダーの信頼のため
平時からの情報開示が必要

ゼネコンを取巻く状況

不審メール（添付ファイル例）

■送信元のドメインのバリエーション
@softbank.ne.jp （ソフトバンク）
@i.softbank.jp （ソフトバンク）
@docomo.ne.jp （NTTドコモ） など

■本文（一行のみ）
・完成図・成績表
・ご確認宜しくお願いします など

ゼネコンを取巻く状況

不審メール（状況例）

■ ばらまき型メール攻撃の状況

月日	サイバー攻撃の概要	確認件数
10月8日～9日	「商品の出荷確認を促す悪質メール」 「複合機からの送信を装ったメール」大量のスパムメール	1,116通
10月27日	「請求書の送付を装った悪質メール」	2049通
10月28日	「ホテル[redacted]を名乗ったメール」	
10月30日	「[redacted]様宛請求書をお送りします」タイトルのメール	
11月20日～24日	「複合機からの送信を装ったメール」大量のスパムメール	494通
12月9日～10日	配達業者を装った「ばらまき型メール」	114通
12月25日～	ウイルスによると思われる機器不具合が複数パソコンで発生	59件
1月19日	「複合機からの自動送信を装った「ばらまき型メール」」	―
1月27日	ウイルスによると思われる機器不具合が複数パソコンで再度発生	15件
2月8日	配達業者を装った「ばらまき型メール」を確認	11通
3月7日	配達業者（日本郵政）を装った「ばらまき型メール」を確認	101通
3月22日	差出人を偽装（宛先と差出人が同じ）して送られたマルウェアメール	9通

ゼネコンを取巻く状況

改ざんサイト（状況例） －偽サイトへ誘導－

『家電　激安』で検索すると・・・

クリックしたら・・・

【偽サイト】

最近の傾向
「単なる詐欺サイト」
→「ランサムウェア植込みサイト」

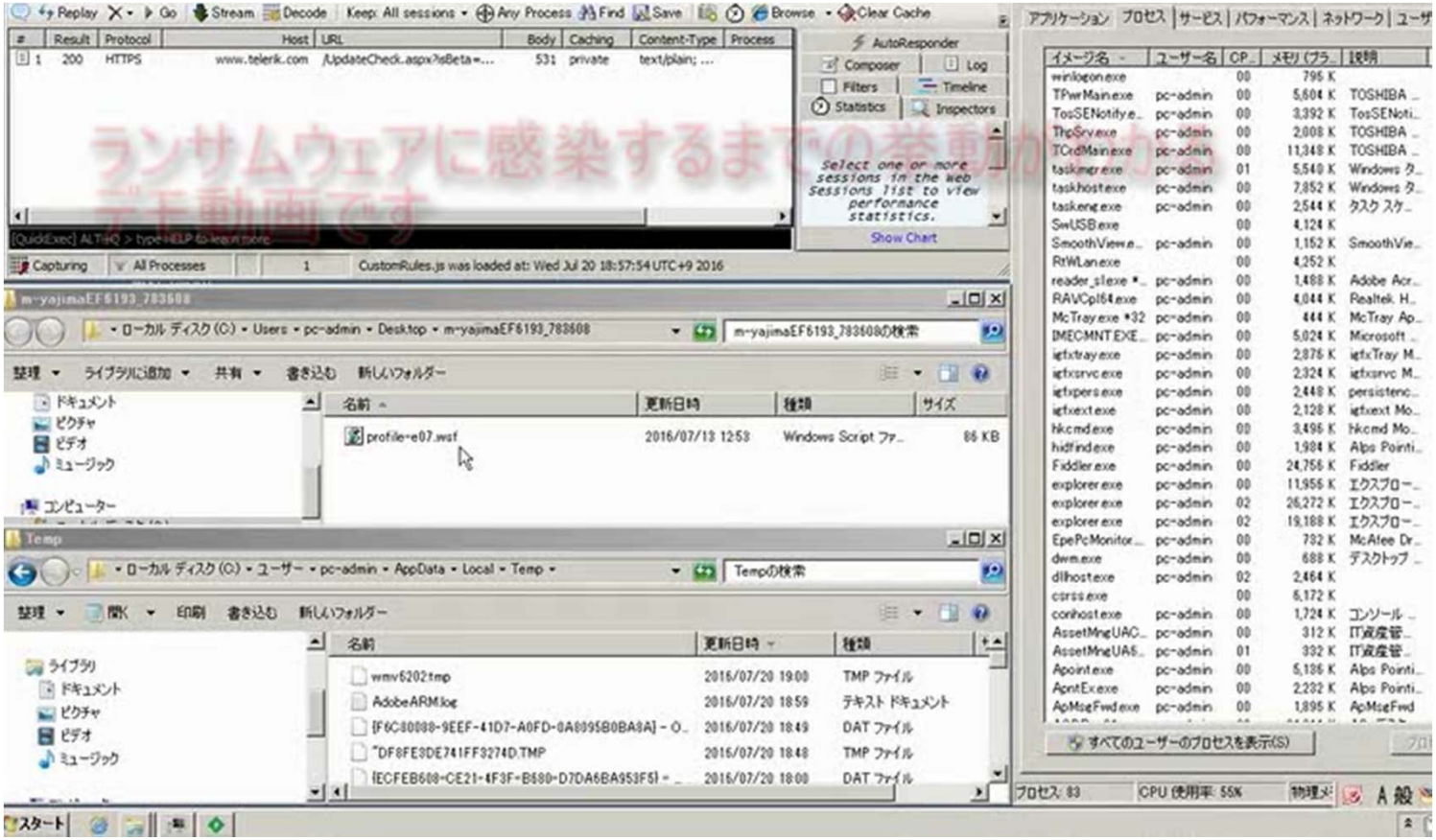
ゼネコンを取巻く状況

改ざんサイト（状況例） －ファーミング詐欺 －

正規のURL入力でも
「詐欺サイト」が表示される
（URL表示はそのまま）

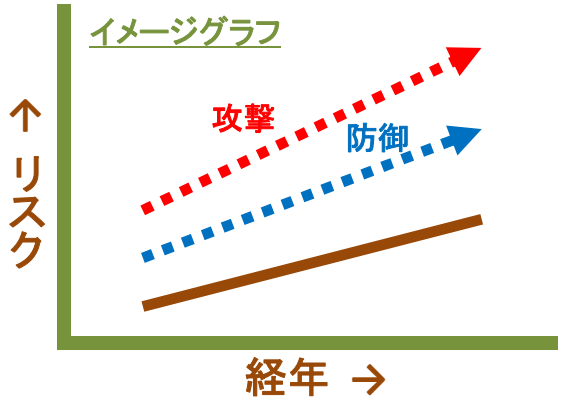
ゼネコンを取巻く状況

ランサムウェア事例



ゼネコンを取巻く状況

○技術的対策は？



クラウド、IoT、AI、、、

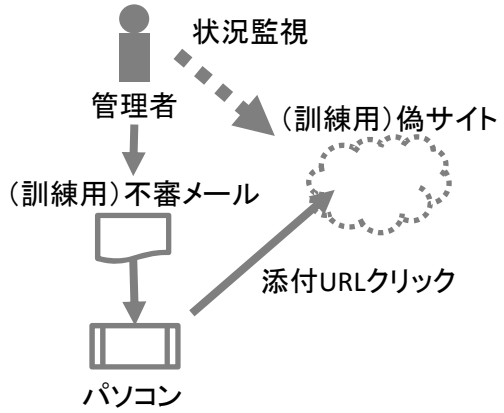
技術進化　攻撃：＋　防御：＋

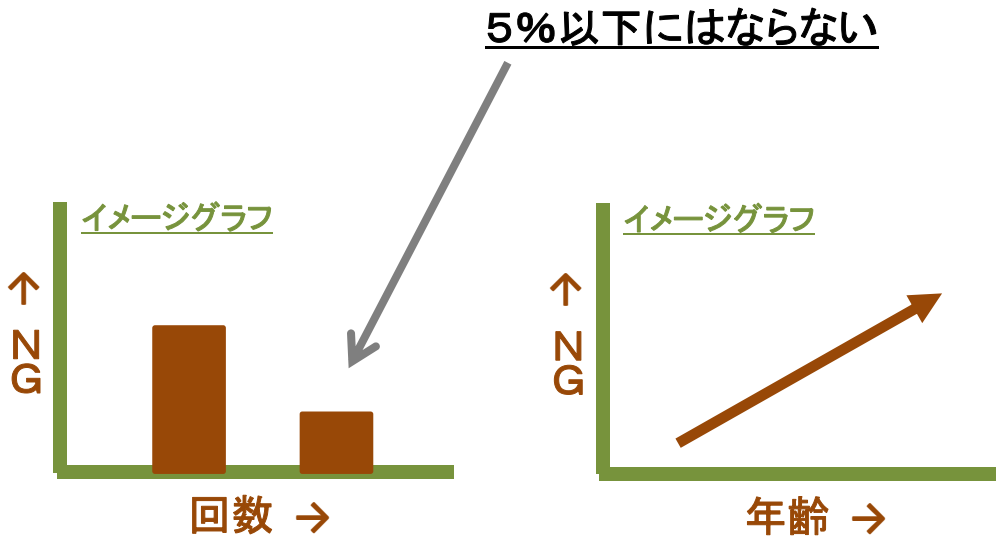
範囲の拡大　攻撃：＋　防御：－

リスクを「ゼロ」に押さえられない！

○人的対策が不可欠！

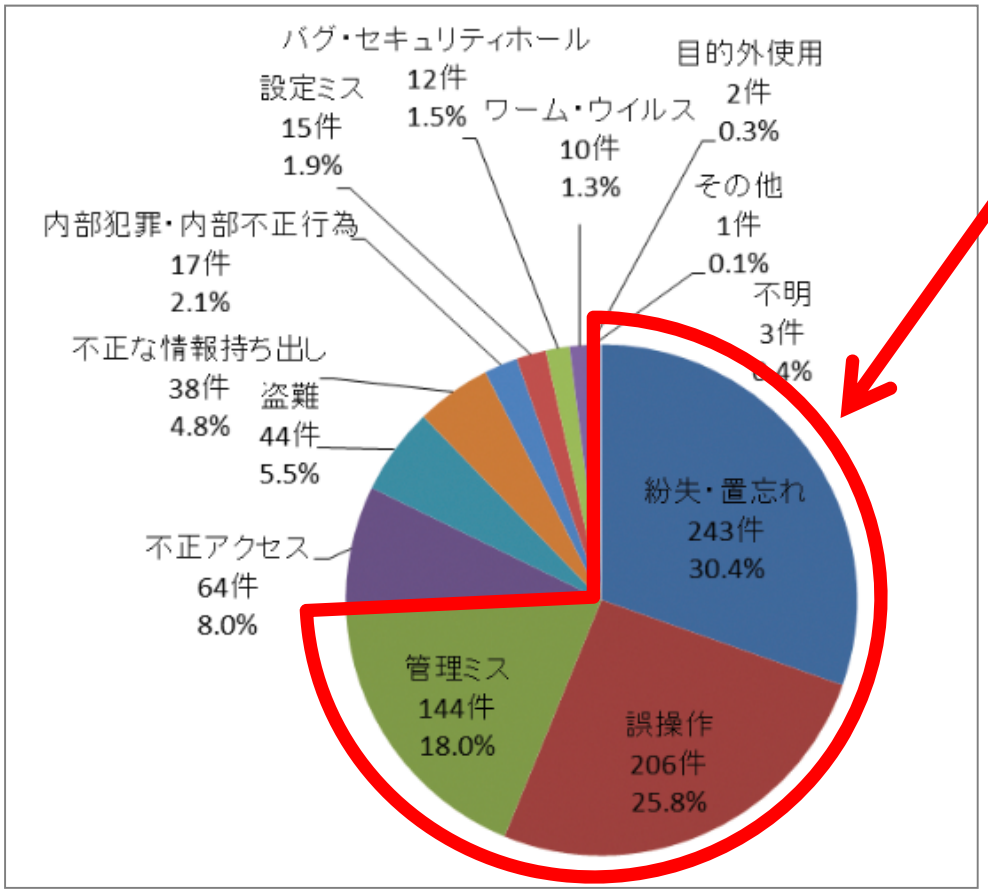
ex.不審メール対策訓練





ゼネコンを取巻く状況

2015年個人情報漏えい事故（JNSA）



人的要素　→　74.2%

建設業の特性

・重層構造（中小規模の会社）
・多くの作業員（短期間）
・職場が顧客の敷地（建物）

協力会社の情報セキュリティ強化が重要

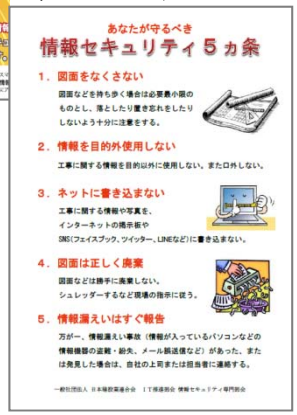
情報セキュリティ専門部会の取組

これまでの取組

継続：教育ツール作成（ポスター、パンフレット、動画、e-learning）

ポスター

リーフレット



e-learning

動画

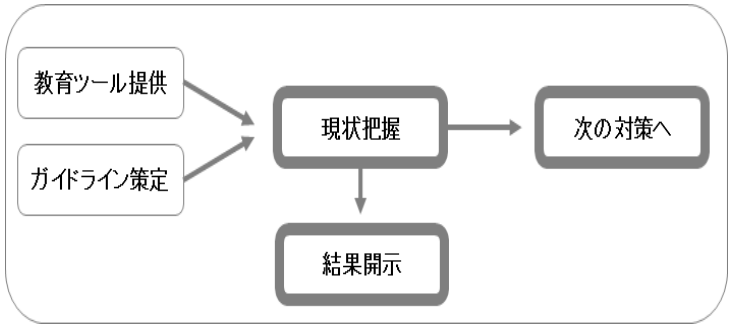
情報セキュリティ専門部会の取組

これまでの取組

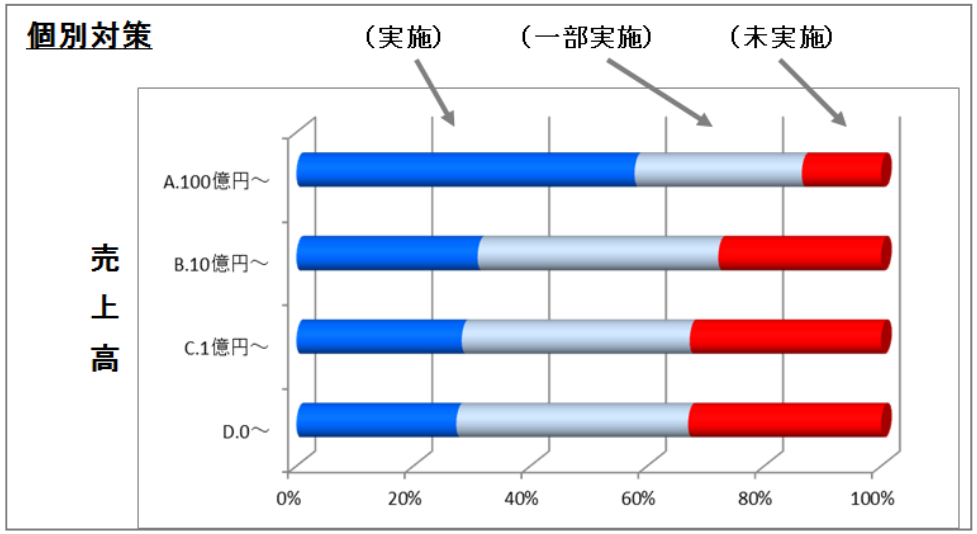
継続：教育ツール作成（ポスター、パンフレット、動画、e-learning）

2014年度：協力会社向けアンケート実施

考え方



アンケート結果



情報セキュリティ専門部会の取組

これまでの取組

継続：教育ツール作成（ポスター、パンフレット、動画、e-learning）

2014年度：協力会社向けアンケート実施

2015年度：

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」 発行

「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　発信

ガイドライン

「はじめに」より抜粋

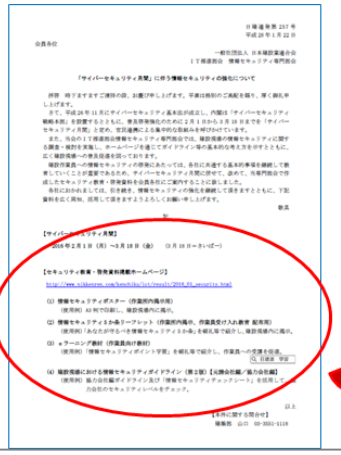
どこでも持ち歩けるスマートデバイスが進化し、建設現場の生産性向上などに役立つツールとして活用が始まっています。

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。

サイバー月間

会員会社への協力依頼（2015/1/22発信）



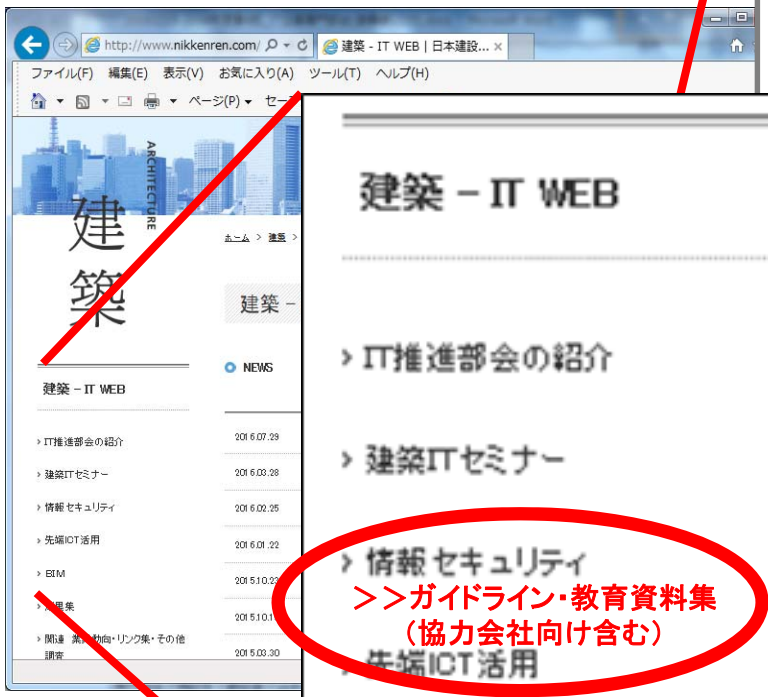
下記ツール類の活用を呼びかけ

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）

情報セキュリティ専門部会の取組

今年度の取組

協力会社向けHPの新設



ガイドライン

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。（位置づけ）
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／協力会社編】
	“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。（位置づけ）
Ⅲ	建設現場ネットワークの構築と運用ガイドライン
	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。（位置づけ）
	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
	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。（位置づけ）

育ツール

	推奨対象者 作業員	社員	経営者	提供元（メディア等）	タイトル
ット		○	○	日建連	情報漏えい防止徹底のお願い
ット	○			日建連	情報セキュリティ5か条リーフレット
ー	○	○		日建連	情報セキュリティポスター「無断で撮らない！　書き込まない！」
ー	○	○		日建連	情報セキュリティポスター「あなたのパソコンが狙われています！」
ー	○	○		日建連	情報セキュリティポスター「あなたの情報が狙われています！」
ング	○	○		日建連	情報セキュリティポイント学習　Ver.1～3
	○	○		日建連	作業所における情報セキュリティ講座
ート		○	○	日建連	情報セキュリティチェックリスト（協力会社用）
注意：以下の教育資料は、リンク先の外部Webサイトに移動します					
	○	○	○	警察庁（専用HP）	情報セキュリティ対策ビデオ
	○	○	○	警察庁（専用HP）	ランサムウェアの説明動画の公開について
		○		パロアルトネットワークス（YouTube）	ランサムウェアLOCKYデモ(字幕あり、音声なし)
動画		○		トレンドマイクロ（YouTube）	不正広告によるランサムウェア感染

情報セキュリティ専門部会の取組

今年度の取組

「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　発信

日建連発第 xxx 号
平成 29 年 1 月 xx 日

会員各位

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

「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について

拝啓　時下ますますご清祥の段、お慶び申し上げます。平素は格別のご高配を賜り、厚く御礼申し上げます。

さて、平成 26 年 11 月にサイバーセキュリティ基本法が成立し、内閣は「サイバーセキュリティ戦略本部」を設置するとともに、普及啓発強化のために 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」と定め、官民連携による集中的な取組みを呼びかけています。

また、当会のＩＴ推進部会情報セキュリティ専門部会では、建設現場の情報セキュリティに関する調査・検討を実施し、ホームページを通じてガイドライン等の基本的な考え方を示すとともに、広く建設現場への普及促進を図っております。

建設作業員への情報セキュリティの啓発にあたっては、各社に共通する基本的事項を継続して教育していくことが重要であるため、サイバーセキュリティ月間に併せて、改めて、当専門部会で作成したセキュリティ教育・啓発資料を会員各社にご案内することに致しました。

各社におかれましては、引き続き、情報セキュリティの強化を継続して頂きますとともに、下記資料を広く周知、活用して頂きますようよろしくお願い申し上げます。

敬具

記

【サイバーセキュリティ月間】

2017 年 2 月 1 日（水）～3 月 18 日（土）　（3 月 18 日＝さいばー）

【セキュリティ強化・啓発資料　掲載ホームページ】

ＩＴ推進部会情報セキュリティ専門部会では、元請会社や協力会社、作業所作業員向けのセキュリティ強化・啓発資料を作成し公開しています。

http://www.nikkenren.com/kenchiku/ict/security/

【セキュリティ月間に向けたセキュリティ強化・啓発資料の活用例】

(1)情報セキュリティポスター
・セキュリティ月間に合わせて現場内に掲示する（ダウンロードしてＡ３版で印刷）
(2)情報セキュリティ５ヶ条（リーフレット）
・朝礼等での内容を紹介する
・ダウンロードのうえ印刷して配布する 等

これら以外にも、「作業所における情報セキュリティ講座 【動画】」や「情報セキュリティチェックシート（2017/1 改定）」を掲載していますので、協力会社への教育と点検にご活用ください。

以上

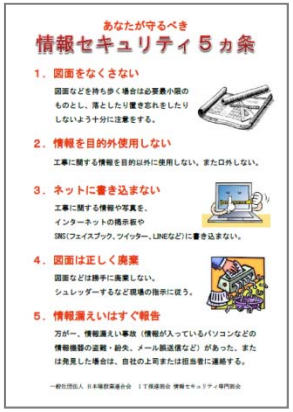
【本件に関する問合せ】
建築部　山口　03-3551-1118

昨年度に引続き、
会員各社へ
「情報セキュリティ対策」を呼びかけます

ポスターの掲示、リーフレットの活用

ポスター

リーフレット



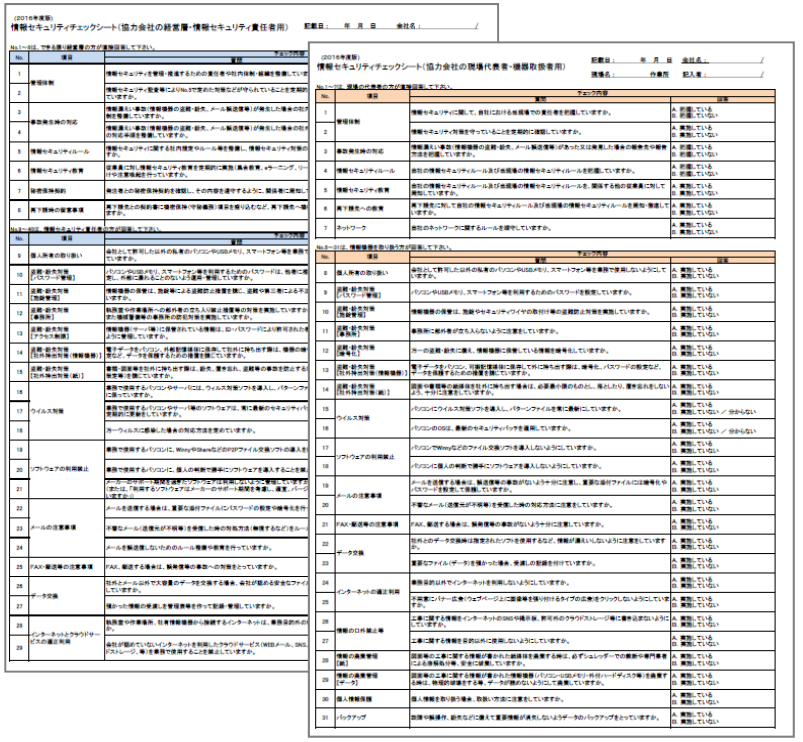
情報セキュリティ専門部会の取組

今年度の取組

既存資料の更新　（最新の情報セキュリティリスクに対して・・）

パンフレット

チェックリスト



まとめ

クラウド、IoT、AI、、、i-Construction、、ICTの利用が増大（データ、機器、業務範囲）

2020東京、攻撃ターゲットのリスク増大

国を挙げての対策、、情報の共有が重要、、経営の課題、、中小企業の強化

建設業の特徴、職場が顧客の敷地（建物）

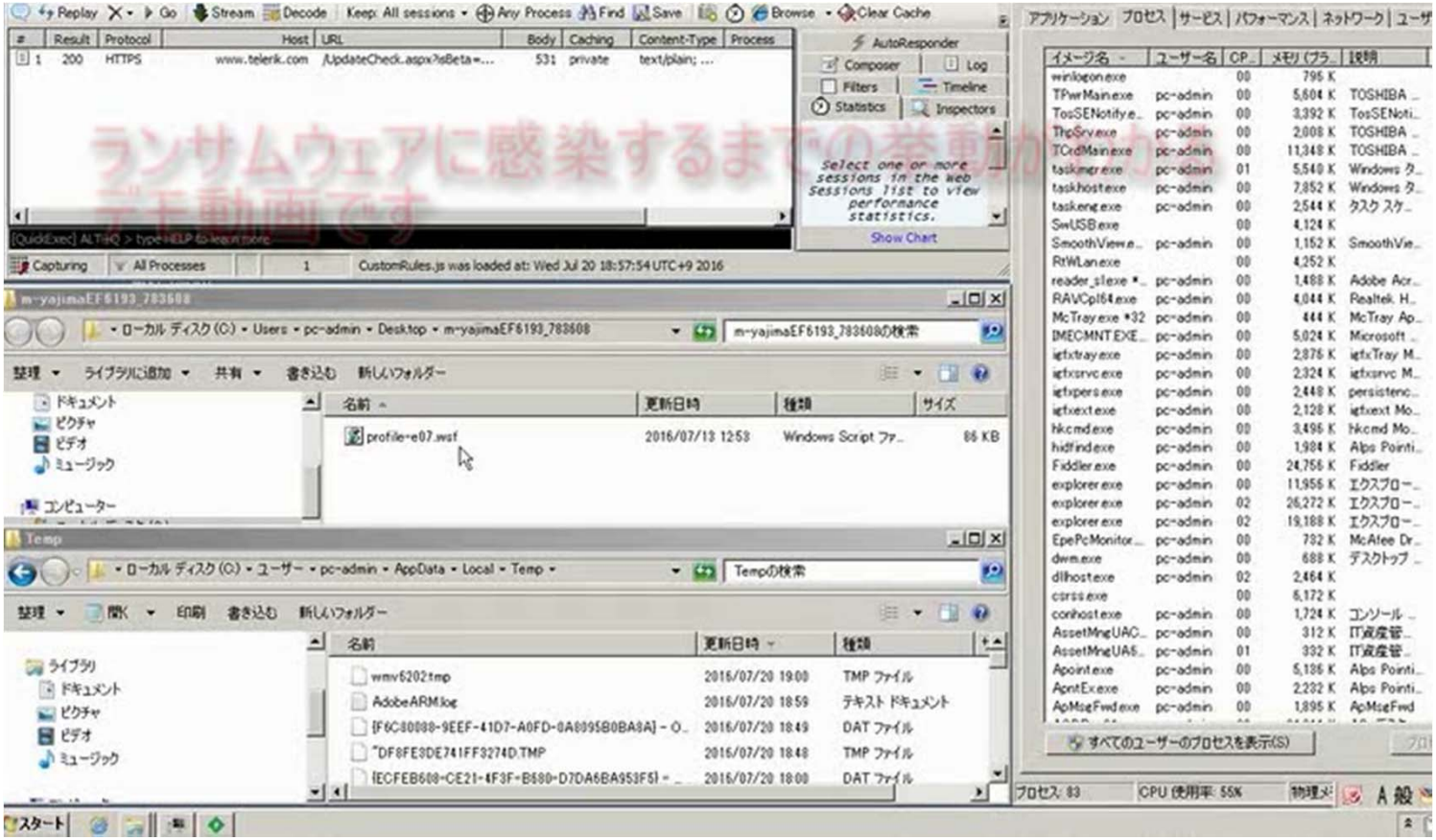
人的要因が3／4、、教育が必要

<u>不審メールは削除！</u>　<u>インターネット上に投稿しない！</u>

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

ランサムウェア事例



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	平峯　元晴	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
石垣　順史	清水建設	山北　岳史	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		