【サイバー攻撃の脅威に備える】

二重脅迫型ランサムウェアの急増等、建設業においても情報セキュリティの取組が増々重要となっています。

協力会社を含めたサプライチェーン全体での取り組みが必須になっており、業界全体での底上げに向けて、日建連での取り組みを紹介します。

情報セキュリティ専門部会

協力会社向け オンラインセミナーを開催 2022/10/19

待ったなし！
サイバー攻撃への対策強化

15:00～15:30　サイバー空間をめぐる脅威の情勢とサイバーセキュリティ対策
(講師：警視庁サイバーセキュリティ対策本部)

15:30～15:50　大成建設でのEMOTETウイルスメール観測状況と、一般的なメールアドレスやパスワード流出の調査例／簡単にできる対策
(講師：ICT推進部会情報セキュリティ専門部会 委員)

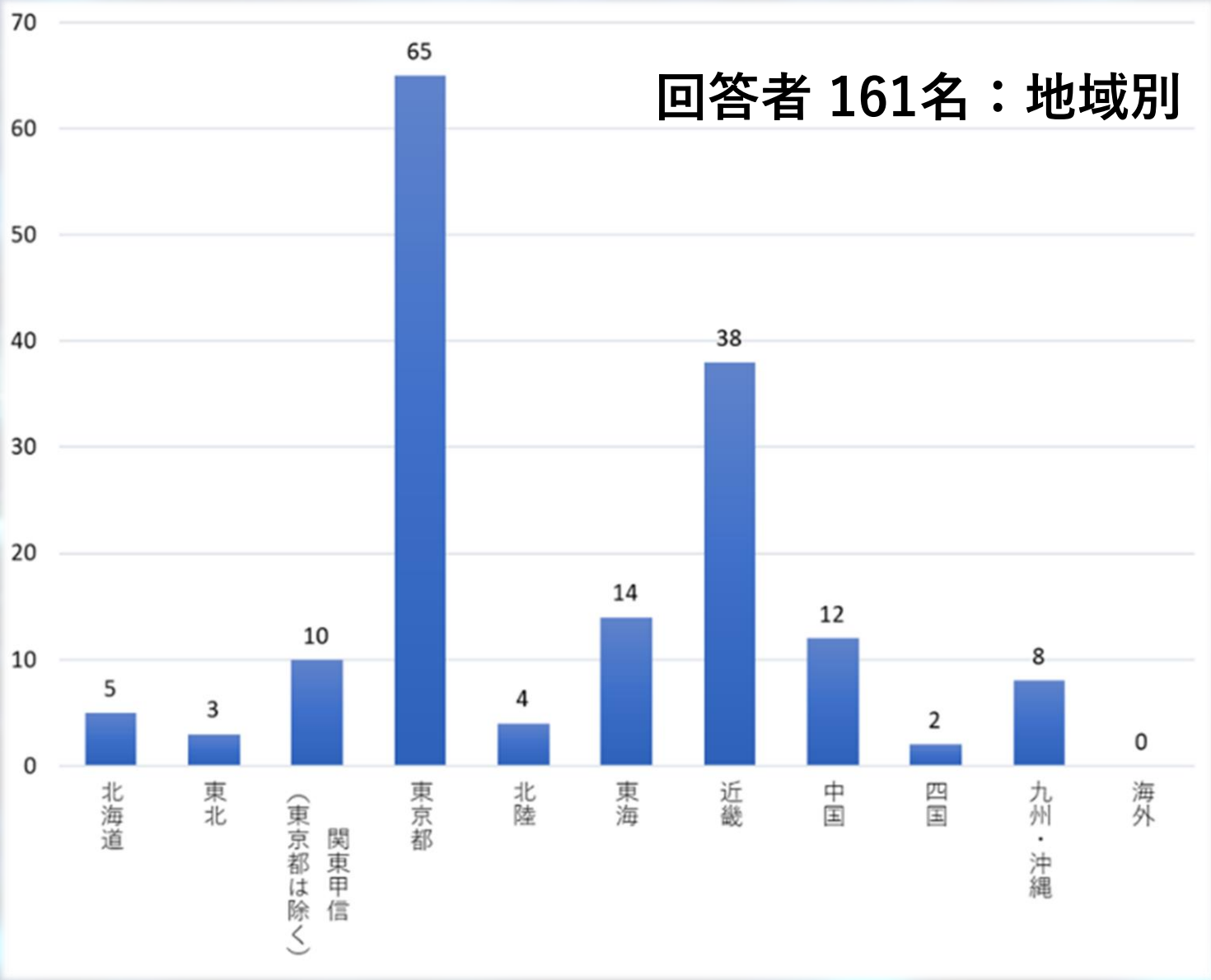
15:50～16:00　休憩

16:00～16:20　サイバーセキュリティお助け隊サービス制度の紹介
(講師：IPA 独立行政法人 情報処理推進機構)

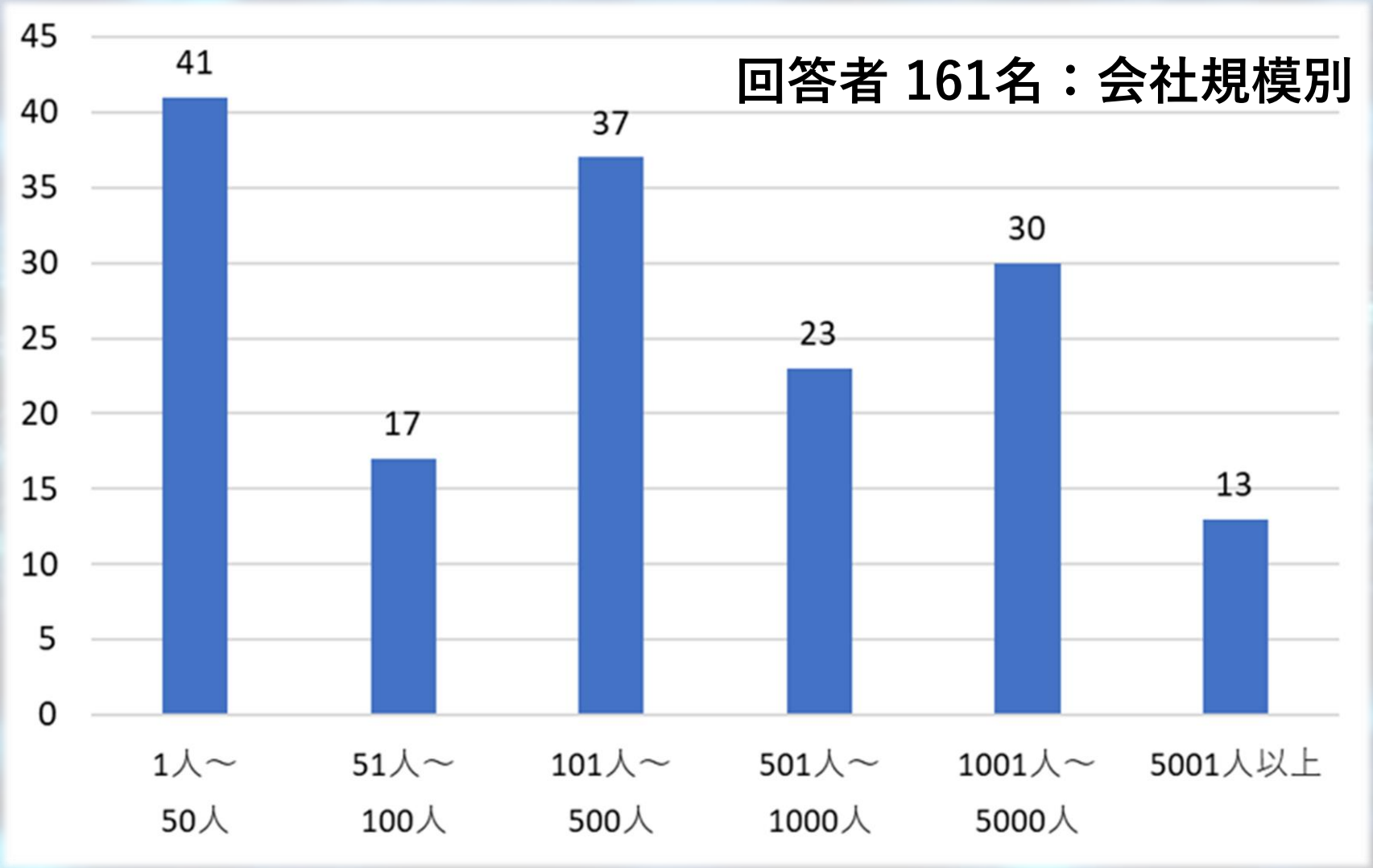
16:20～16:30　当専門部会で作成したセキュリティ対策・教育啓発資料の紹介
(講師：ICT推進部会情報セキュリティ専門部会 主査)

16:30～16:45　質疑応答

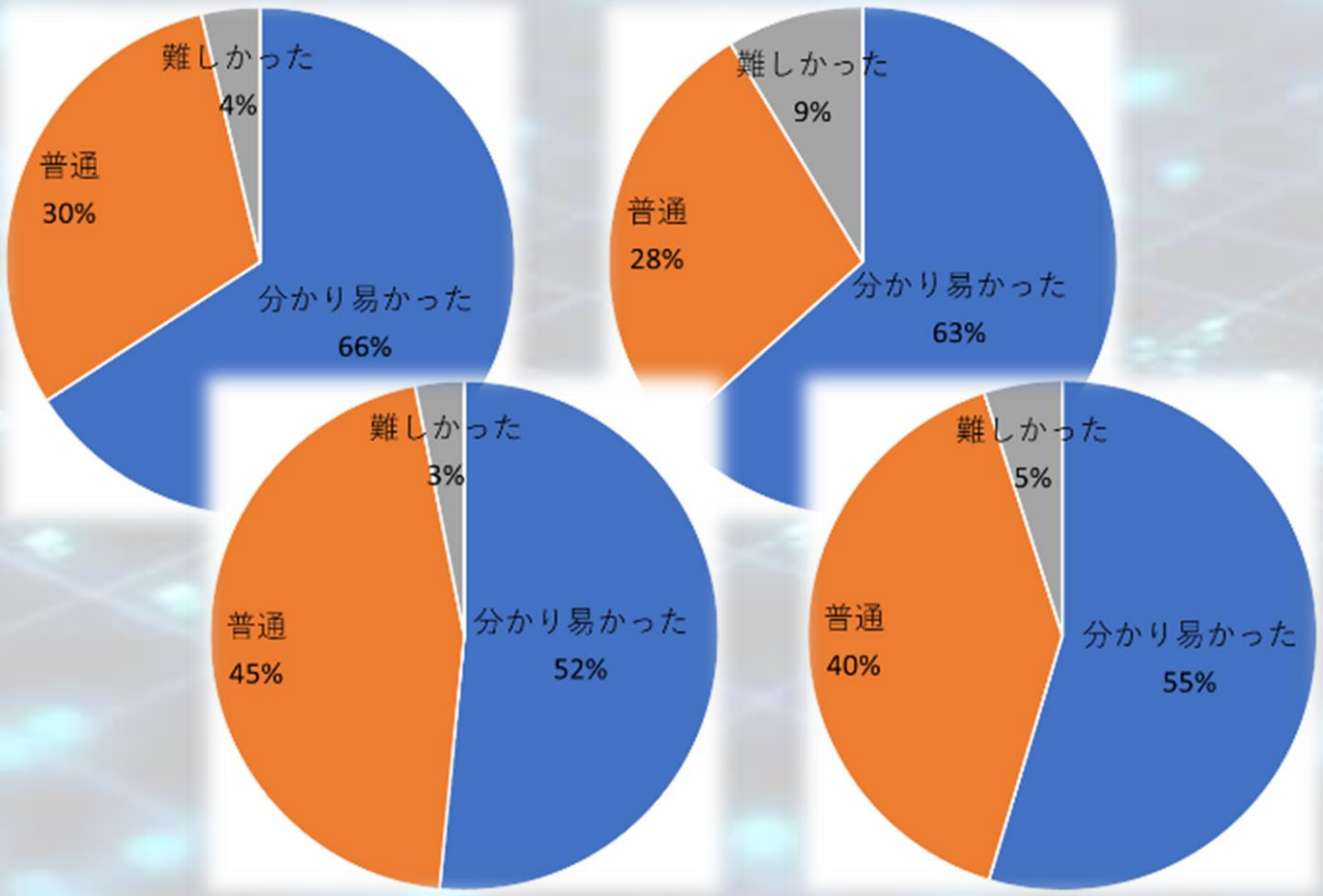
協力会社向け オンラインセミナーを開催 2022/10/19



協力会社向け オンラインセミナーを開催 2022/10/19



協力会社向け オンラインセミナーを開催 2022/10/19



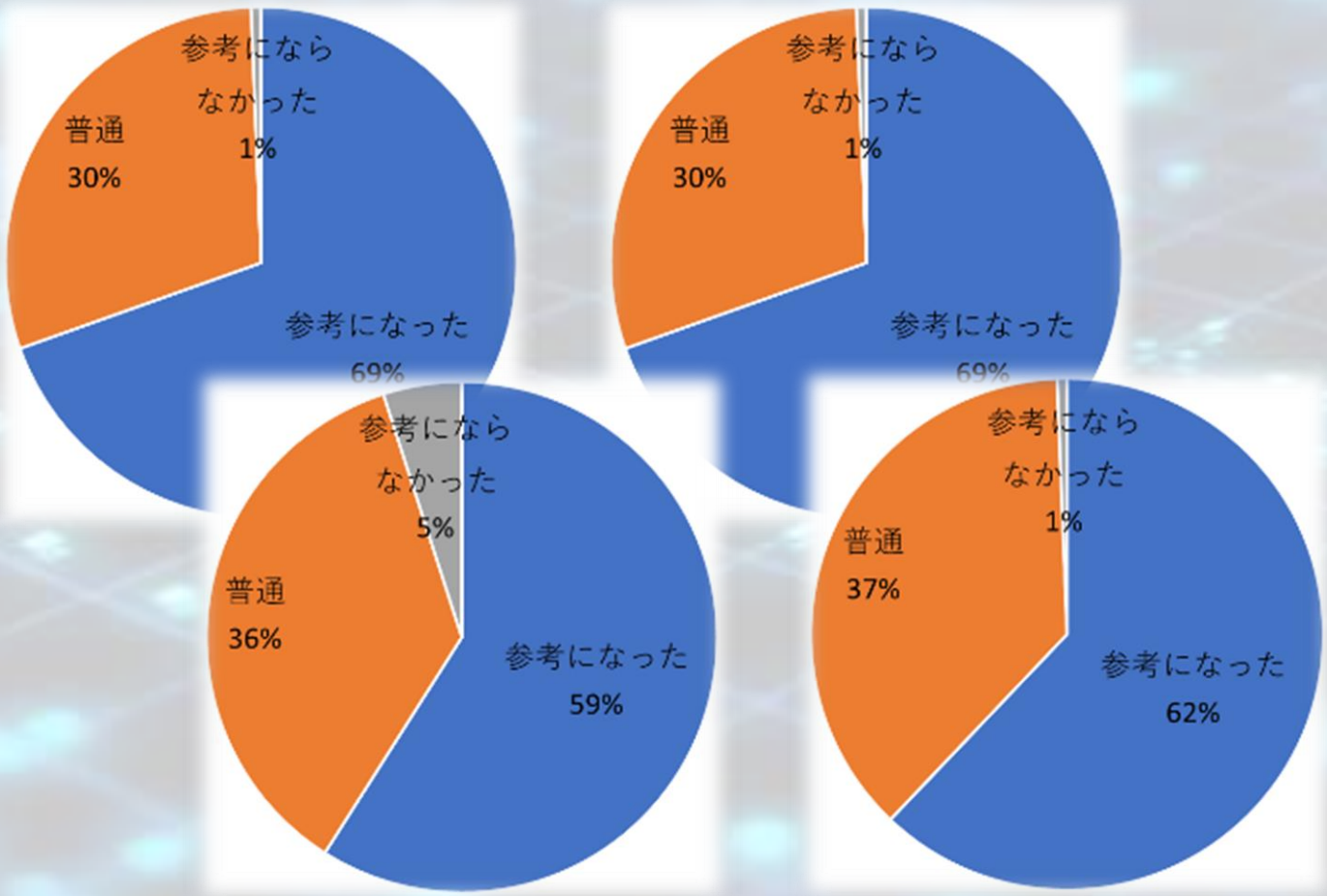
講演内容別_集計
わかりやすさ

分かり易かった

普通

難しかった

協力会社向け オンラインセミナーを開催 2022/10/19



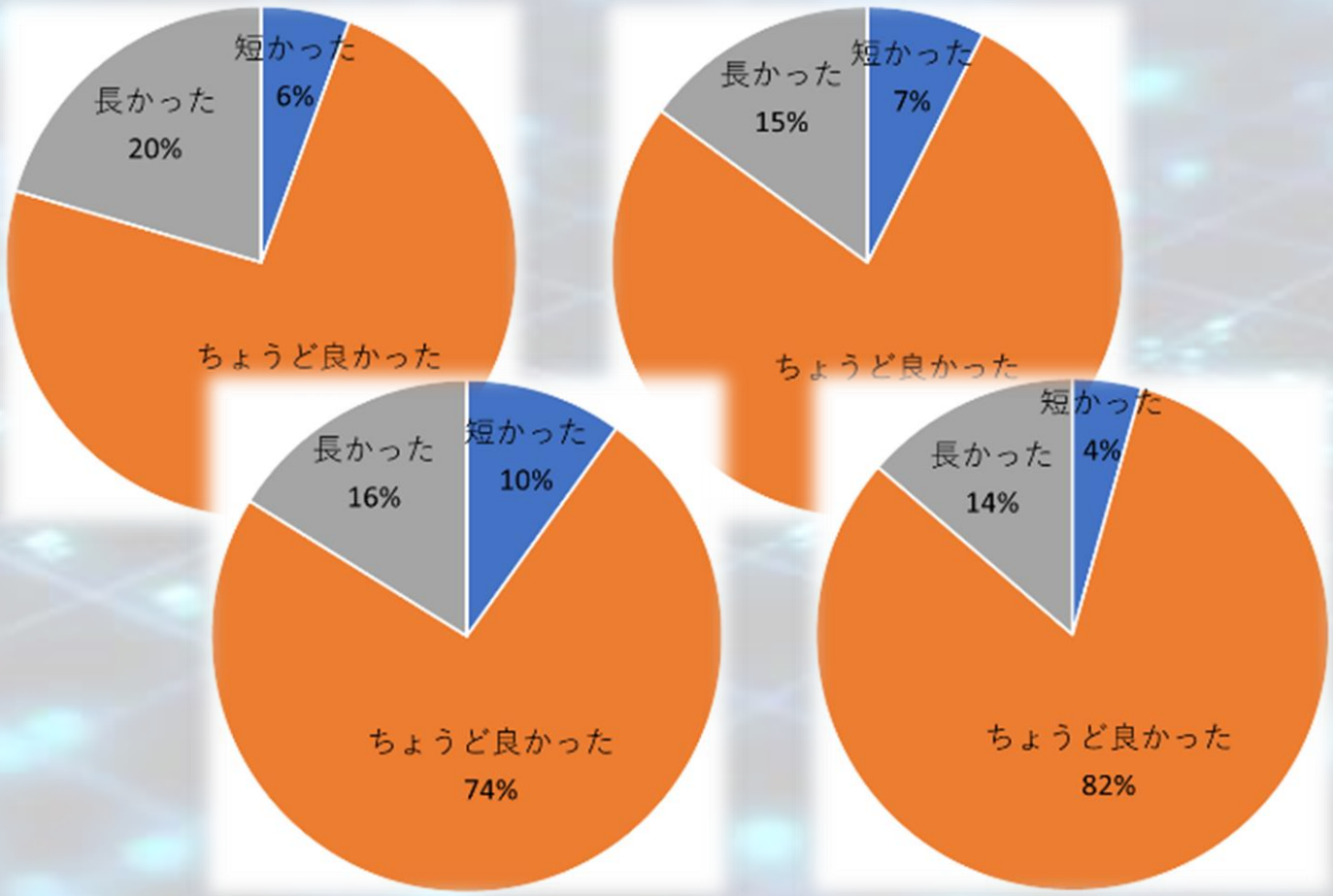
講演内容別_集計
参考になるか

参考になった

普通

参考にならなかった

協力会社向け オンラインセミナーを開催 2022/10/19



講演内容別_集計
時間

短かった

ちょうど良かった

長かった

サイバー月間（２月１日～３月１８日サイバーの日）

NICS：内閣サイバーセキュリティセンター　ＨＰ

サイバー月間（２月１日～３月１８日サイバーの日）

我が国を始め世界中で、ランサムウェアを始めサイバー攻撃による被害が多発し、社会や経済にも大きな影響が及んでいます。

皆様お一人お一人がサイバー空間を安全・安心に利用していただくために、「適切なパスワードを使う」、「最新版のソフトウェアを使う」、「困ったときは各種相談窓口に相談する」など、基本的な対策を徹底していただくことがとても重要です。

基本的な対策を「サイバーセキュリティ対策９か条」としてまとめ・・・

サイバーセキュリティの向上に「全員参加」で取り組んで参りましょう。

首相官邸　ＨＰ

サイバー月間（２月１日～３月１８日サイバーの日）

各項目を動画で解説

NICS：内閣サイバーセキュリティセンター　ＨＰ

サイバー月間（２月１日～３月１８日サイバーの日）

日建連発 181 号
2023 年 1 月 27 日

会員各位

一般社団法人日本建設業連合会
建築生産委員会 ICT 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、建設業においてはＤＸ推進等に伴うＩＣＴ活用が益々拡大されることになり、情報セキュリティの重要性がさらに増していくと考えられます。特に最近では「二重脅迫型ランサムウェア」が急増しておりサイバー攻撃のリスクが急速に高まっています。政府は、サイバーセキュリティに関する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。

ICT 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。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合わせて、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。

会員各社におかれましては、下記資料を広く周知、活用をして、協力会社の指導を含め、情報セキュリティの強化を継続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】

2 月 1 日~3 月 18 日　（3 月 18 日＝サイバー）

【情報セキュリティ教育・啓発資料掲載ホームページ】
https://www.nikkenren.com/kenchiku/ict/security/guideline.html

（今回新規作成）
（1）情報セキュリティ啓発ポスター（日本語版＋英語版）：「サイバー攻撃注意報」
（使用例）A3 判で印刷し、建設現場内、および事務所内に掲示。
（2）情報セキュリティ教育・研修用動画：「二重脅迫型ランサムウェアの予防と対処」

以上

■本件に関する問合せ先
建築生産委員会 ICT 推進部会事務局（担当：齋藤）　kenit@nikkenren.or.jp
※事務所不在の場合がありますので、メールでのご連絡をお願いいたします。

資料

「サイバー攻撃注意報」ポスター（日本語版）
推奨対象者：作業員、社員
提供元：日建連

ダウンロード

「サイバー攻撃注意報」ポスター（英語版）
推奨対象者：作業員、社員
提供元：日建連

ダウンロード

3）動画：「二重脅迫型ランサムウェアの予防と対処」

動画公開ページ（Youtube & ダウンロード）

日建連　ＨＰ

サイバー月間（２月１日～３月１８日サイバーの日）

サイバー月間（２月１日～３月１８日サイバーの日）

パンフレット：IoTセキュリティについて

IoT（Internet of Things）セキュリティについて

（2）最低限の対処…>>>

（3）IoT に関するセキュリティ対策全体の詳細…>>>

（4）実際に被害が発生してしまったら…>>>

（5）「サンプル」チェック サイト で確認 >>>

パンフレット：IoTセキュリティについて

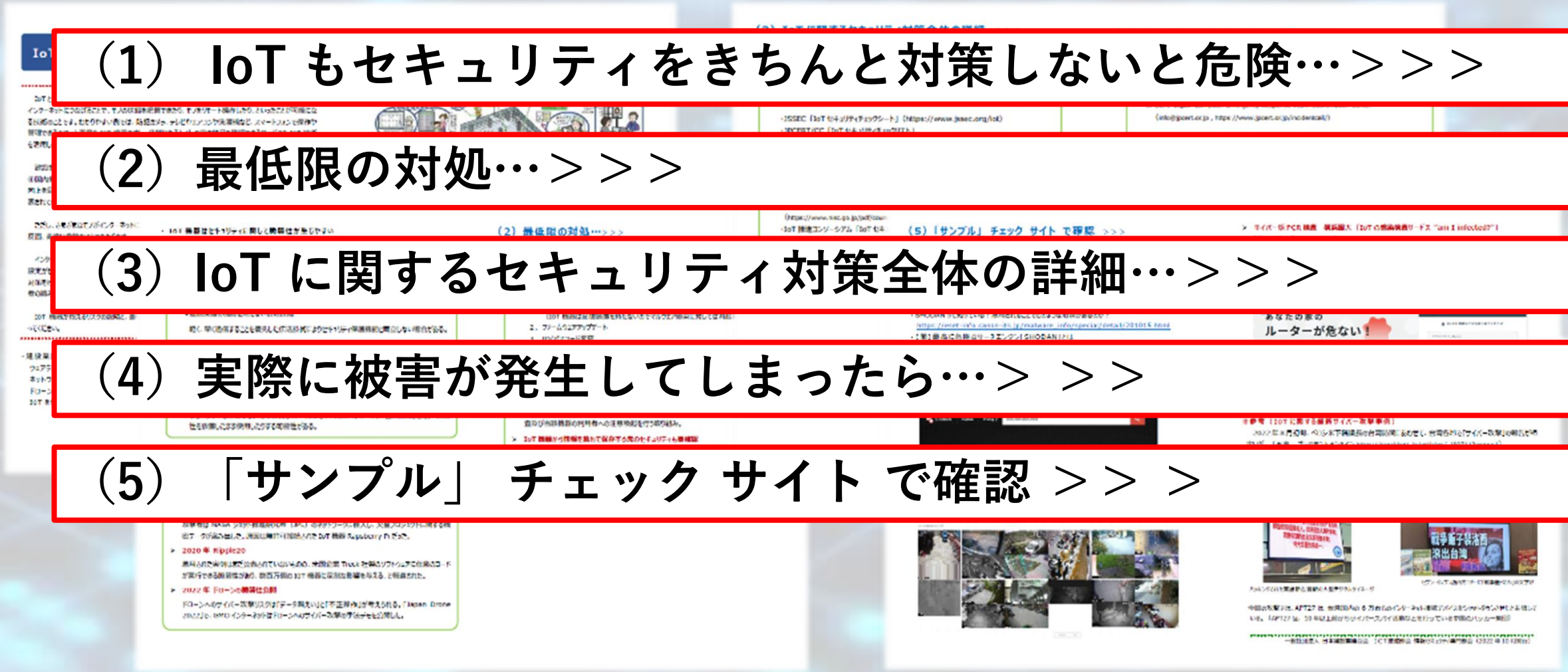
（1） IoT もセキュリティをきちんと対策しないと危険…＞＞＞

（2） 最低限の対処…＞＞＞

（3） IoT に関するセキュリティ対策全体の詳細…＞＞＞

（4） 実際に被害が発生してしまったら…＞ ＞＞

（5） 「サンプル」 チェック サイト で確認 ＞＞ ＞



（2）最低限の対処…＞＞＞

➢ NICT（国立研究開発法人情報通信研究機構）
「すぐできるIoT機器セキュリティ対策６」
（「サイバー攻撃の動向とセキュリティ研究2021」セミナー）

1．IoT再起動
（IoT機器は記憶装置を持たないのでマルウェア感染に対しては再起動で駆除できる）
2．ファームウェアアップデート
3．ID/パスワード変更
4．インターネット側からのアクセス拒否設定
5．ゲートウェイ機器の内側に設置
6．古い機器は買い替え（自動アップデート機能がない機器はNG）

セキュリティガイドライン

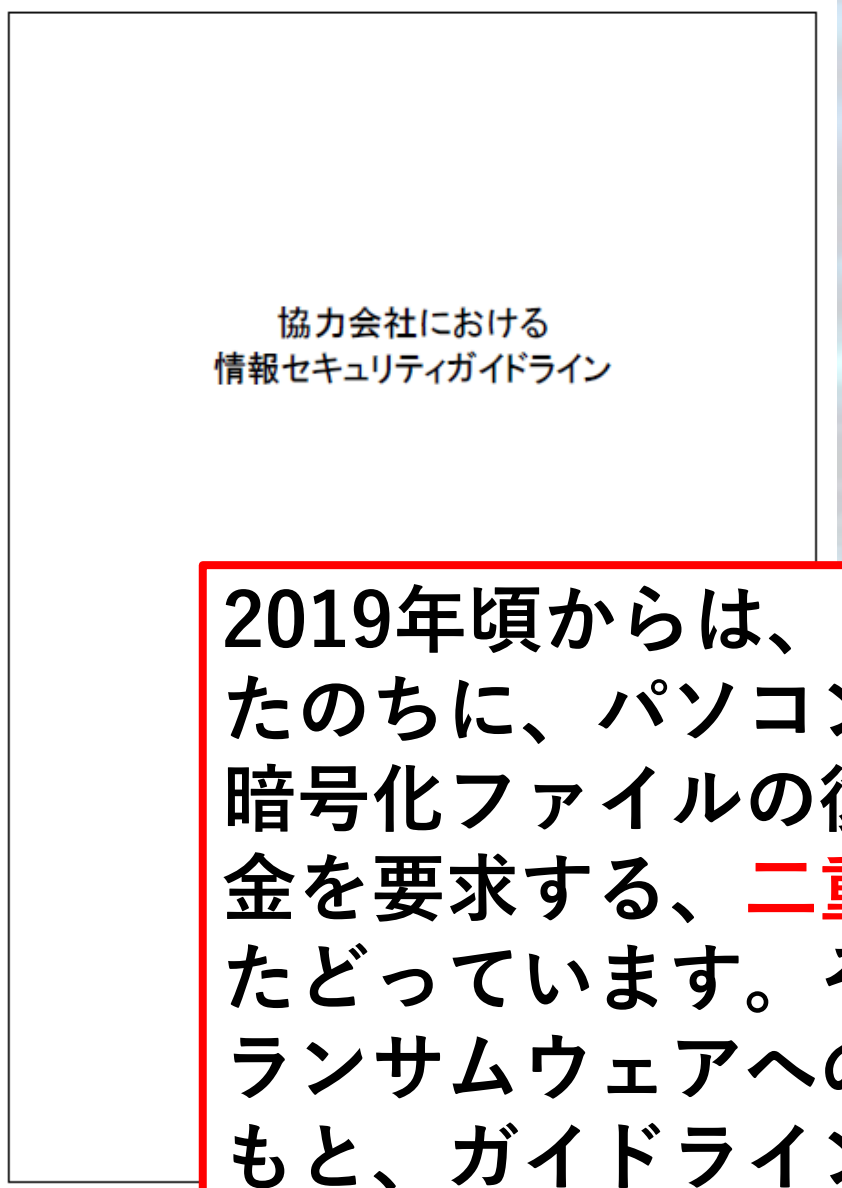
「協力会社における情報セキュリティガイドライン」改定

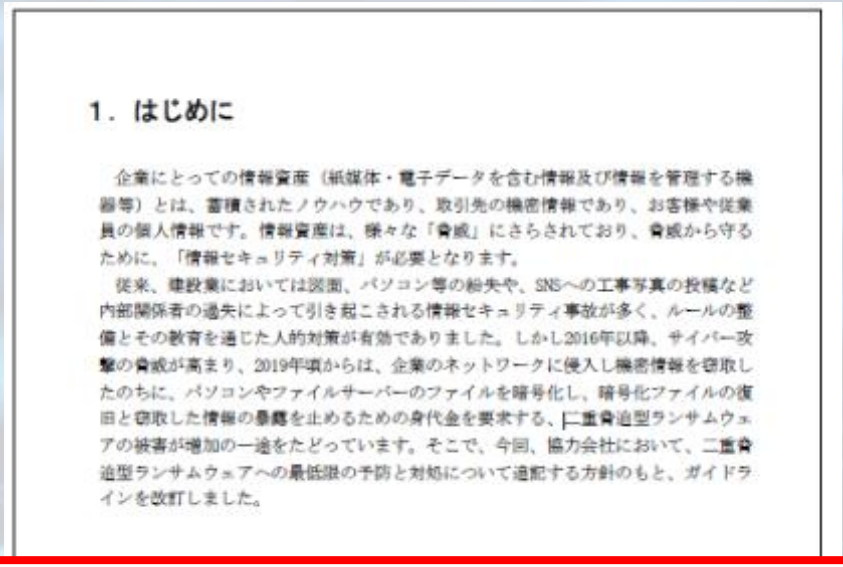
ガイドライン

› ガイドラインの位置づけ

I	建設現場における情報セキュリティガイドライン：2020/11 改訂
	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	元請会社における情報セキュリティガイドライン：2020/11 改訂
	元請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
III	協力会社における情報セキュリティガイドライン：2020/11 改訂
	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：2020/11 改訂
	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：2021/11 改訂
	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

セキュリティガイドライン





2019年頃からは、企業のネットワークに侵入し機密情報を窃取したのちに、パソコンやファイルサーバーのファイルを暗号化し、暗号化ファイルの復旧と窃取した情報の暴露を止めるための身代金を要求する、**二重脅迫型ランサムウェアの被害が増加**の一途をたどっています。そこで、今回、協力会社において、二重脅迫型ランサムウェアへの**最低限の予防と対処について追記する**方針のもと、ガイドラインを改訂しました。

2）ランサムウェアなどのサイバー攻撃を想定した追加施策

【侵入予防】

① 自社のインターネットの出入口を確認
「SHODAN」等のツールで自社のインターネット出入口の
不要なポートが開かれていないかを確認
RDP（ リモートデスクトップ）や インターネットVPN を確認

② 出入口のセキュリティ強化
不要なポートを閉じる／制限する／脆弱性を無くす

③ 本格調査と本格対策
セキュリティ専門会社によるペネトレーション（侵入）テスト
セキュリティ専門会社によるアセスメント・アドバイス

2）ランサムウェアなどのサイバー攻撃を想定した追加施策

【感染予防】

① 中小企業向け 「サイバーセキュリティお助け隊」制度の活用

② EDR（ふるまい検知型ウイルス対策ソフトウェア）の導入

出入口対策やウイルス対策ソフトでも侵入を防止できない最近のランサムウェア等の強力なマルウェアが、サーバーやパソコンで活動することを阻止する。侵入を前提とした最後の砦となるツール。

- ランサムウェアによる暗号化防止
- 社内に侵入するためのバックアドアを仕掛ける マルウェアの感染防止

③ Windows Active Directory ドメイン管理者の権限管理

- 一般ユーザーにローカル管理者権限を与えない

2）ランサムウェアなどのサイバー攻撃を想定した追加施策

【攻撃に備えて実施しておくべきこと】

① バックアップ取得と復旧訓練
　オンラインまたはオフラインバックアップを
　複数とることが望ましい
　定期的な復旧訓練で復旧できることを確認しておくことが必要

② サーバー・ネットワーク機器・パソコン 等の監査ログの取得

③ サイバーセキュリティ保険への加入検討

２）ランサムウェアなどのサイバー攻撃を想定した追加施策

【実際に被害が発生してしまったら】

① 通報・相談・アドバイス

警察

IPA 情報処理推進機構 情報セキュリティ安心相談窓口

JPCERT　Coordination Center

② 専門会社へ調査・対処の依頼

サイバーセキュリティ事故 緊急対応」で検索し、対応できる

セキュリティ専門会社に依頼する

セキュリティガイドライン

～二重脅迫型ランサムウェアの予防と対処について～

2019 年頃から、企業のネットワークに侵入し機密情報を窃取したうえに、パソコンやファイル
を暗号化し、暗号化ファイルの復旧と窃取した情報の暴露を止めるための身代金を要求す
ランサムウェアの被害が発生し始めました。2020 年以降大企業が被害に遭い、高額な身
たことが大きく報道されました。

二重脅迫型ランサムウェアの被害は増加の一途をたどっており、2021 年 6 月には、世界
1,210 件の被害が発生しました。（出典：Check Point Software Technologies「Ransomware a
Surge, hitting a 93% increase year over year」）
また、2021 年の身代金支払い総額は 2 兆円に達するとみられています。

「うちは暴露されて困るような機密情報はないし…」と思われるかもしれませんが、攻撃者は
狙うのではなく、サプライチェーンを構成している、攻撃しやすいセキュリティ対策の甘い中小
げており、日々様々な企業で不正アクセスを受けたとのニュースが報道されています。

外部からの侵入防止に関して、セキュリティ対策を全くとっていない状況も見受けられます。
は、サイバー攻撃を受けていないのはたまたま攻撃者の網にかかっていないだけなのです。

二重脅迫型ランサムウェアへの最低限の予防と対処について記載しますので、確認・対策を

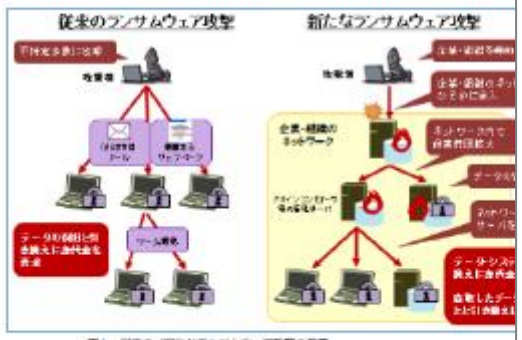


図1　従来の／新たなランサムウェア攻撃の概要

（出典：IPA（独立行政法人情報処理推進機構）「【注意喚起】事業継続を脅かす新たなランサム

（1）侵入予防…>>>

・まずは、自社のインターネットの出入口を確認してみましょう。（簡易な調査）

➢ "SHODAN"で自社のインターネット出入口が外からどう見えているか調べてみる。

・調査（本格調査）

➢ セキュリティ専門会社によるペネトレーション（侵入）テスト
- 専用のツールや高度な知識を有する専門家により実際に侵入や攻撃
- 費用　数十万円～（自動テストツール）　百万円～（ホワイトハッ
様のテスト）

・対策（本格対策）

➢ セキュリティ専門会社によるアセスメント・アドバイス
- ペネトレーションテストの結果や、ネットワーク環境や機器構成の詳細
リスクを見える化し、対策のアドバイスを受ける。
- 費用　数百万円～

（2）感染予防…>>>

➢ 中小企業向け「サイバーセキュリティお助け隊」
- https://www.ipa.go.jp/security/keihatsu/sme/otasuketai/index.ht

➢ EDR（ふるまい検知型ウイルス対策ソフトウェア）の導入
- ランサムウェアによる暗号化防止
- 社内に侵入するためのバックドアを仕掛けるマルウェアの感染防止

➢ Windows Active Directory ドメイン管理者の権限管理
- ローカル管理者権限を与えている場合は外す。ドメイン管理者権限
きることを制限する。

（3）攻撃に備えて実施しておくべきこと…>>>

➢ バックアップ取得と復旧訓練
ランサムウェアに感染した場合、バックアップもオンラインのものは暗号化
ンバックアップ 2 種、オフラインバックアップ 1 種の計 3 種類のバックアッ
また、復旧訓練をおこなっていないと、実際バックアップから戻らない場
旧できることを確認しておく必要がある。

➢ サーバー・ネットワーク機器・PC 等の監査ログ取得
攻撃を受けたことが判明しセキュリティ専門会社に調査を依頼しても、
合調査をすることができないため、監査ログを取得するよう設定する。

➢ サイバー保険加入検討
損害賠償・調査や対処の費用・自社の喪失利益、を補償するサイバ
いるので、加入を検討する。

（4）実際に被害が発生してしまったら…>>>

・ランサムウェアの被害に遭った場合、身代金を支払っても復旧できるとは限りません。まずは信

（5）SHODAN サンプル…>>>

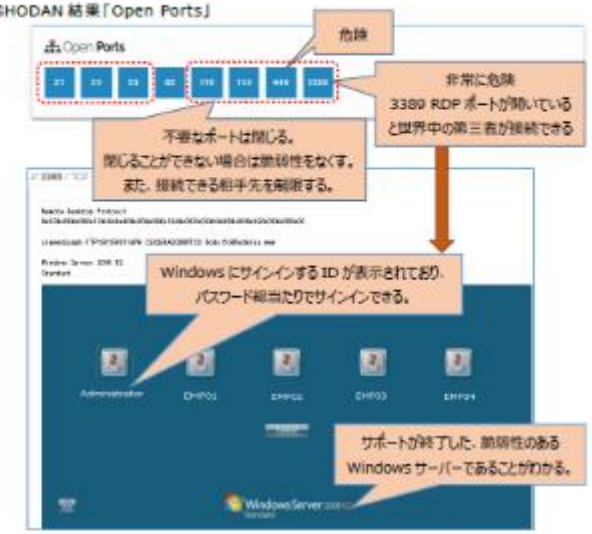
SHODAN の利用にあたっては、IPA（情報処理推進機構）発行の「増加するインターネット接続機器の不適切な情報公開とその対策」を必ず参照してから実施してください。
https://www.ipa.go.jp/about/technicalwatch/20140227.html
また、社内ネットワークから SHODAN へのアクセスを禁止している企業もあるので、アクセスできない場合は自社のセキュリティ担当部署に相談してください。

・自社のグローバル IP アドレスの確認　https://www.cman.jp/network/support/go_access.cgi

・SHODAN　https://www.shodan.io

・SHODAN 結果表示

・SHODAN 結果「Open Ports」



・SHODAN 結果「Vulnerabilities（脆弱性）」

情報セキュリティ　ガイドライン・教育資料集

日建連→建築→ IT-WEB →【ガイドライン・教育資料集】

情報セキュリティリスクの低減に向けて

安心して、ICT活用を推進するために
皆様のご協力をお願い致します

情報セキュリティ専門部会

安藤ハザマ	高馬 洋一	東急建設	藤井 隆行
竹中工務店	豆腐谷 洋一	戸田建設	藤田 直紀
大林組	杉山 宜督	フジタ	山口 正志
鹿島建設	田口 慶	前田建設工業	滝沢 強
清水建設	市橋 章宏	三井住友建設	仙波 幹徳
大成建設	葛原　徹		