令和 2 年 4 月 30 日

テレワークを行う上での中小企業等の経営者の心構え5箇条を配信！

～地域のキーパーソンに聞く、新型コロナウイルス禍におけるサイバーセキュリティ対策～

関西サイバーセキュリティ・ネットワーク事務局（近畿経済産業局、近畿総合通信局及び一般財団法人関西情報センター）では、関西を拠点として活躍する有識者に電話会議形式でご意見を頂き、テレワークにおける中小企業等の経営者の心構え5箇条についてまとめましたので、2020 年サイバーセキュリティ特別企画として配信します。

なお、同有識者から寄稿いただいた 60 秒で読むことができるコラム記事を、先行配信しています。

1. 趣旨

現在、新型コロナウイルスの感染拡大に伴って、経済や社会にさまざまな影響が波及しています。在宅勤務やテレワークを実施する企業が増えておりますが、この混乱に乗じて、サイバー攻撃、フィッシングメールや不正アプリ、フェイクニュースなどが増加しており、サイバーセキュリティ対策の必要性が高まっています。

また、テレワークは、新型コロナウイルス感染症が収束した後も、新しいビジネスの創出、時間・空間の有効活用につながり、多様化するライフスタイルの実現に寄与するものと考えられますので、今後とも重要な働き方のひとつです。

このような状況に鑑み、関西サイバーセキュリティ・ネットワーク事務局（近畿経済産業局、近畿総合通信局及び一般財団法人関西情報センター）は、中小企業等の経営者に向けて、サイバーセキュリティに対する心構えを「テレワークを行う上での中小企業等の経営者の心構え5箇条」として配信します。

なお、同有識者から寄稿いただいた 60 秒で読むことができるコラム記事を先行配信し、簡潔かつ分かりやすい形で、中小企業のセキュリティ対策のヒントを提供しています。

別添資料：「テレワークを行う上での中小企業等の経営者の心構え5箇条」

＜下記 HP にて公開＞

〇近畿経済産業局 HP

https://www.kansai.meti.go.jp/2-7it/k-cybersecurity-network/interview2020/keypersonSP.html

〇近畿総合通信局 HP

（5箇条） https://www.soumu.go.jp/main_content/000685459.pdf

（先行配信コラム） https://www.soumu.go.jp/soutsu/kinki/01sotsu07_01001651.html

2. ご協力いただいた有識者（氏名 50 音順）

大阪大学　情報セキュリティ本部　猪俣　敦夫　教授
立命館大学　情報理工学部　上原　哲太郎　教授
神戸大学大学院　工学研究科　森井　昌克　教授

（参考1）国内での新型コロナウイルス禍に乗じたサイバー攻撃事例

- 「マスクが購入できる通販サイトがある」というSNSの投稿を見て、通販サイトから購入したが、不審なサイトと思われるとの相談があった。
- 新型コロナウイルスを口実に「助成金があるので、個人情報や口座情報を教えてほしい」等の相談事例があった。
  【転載元】http://www.kokusen.go.jp/（(独)国民生活センターHPより）
- 「偽サイトから「ZOOM」をインストールしたら、セキュリティ警告が表示され、表示先電話番号に電話をしたらサポート料金を請求された」という複数の相談があった。
  【転載元】https://twitter.com/ipa_anshin/ （(独)情報処理推進機構　公式ツイッターより）

（参考2）海外における新型コロナウイルス禍に乗じたサイバー被害

- 3月上旬、スペインの病院がランサムウェア「NetWalker」の攻撃を受けITインフラの一部が使用不能に。スペイン病院初のサイバー被害事例。
- 3月10日、イリノイ州Champaign- Urbana地区の公衆衛生局のHPがランサムウェア攻撃を受けダウン。
- 3月12-13日、チェコ内でコロナ対応を担っていたBrno大学の病院がサイバー攻撃を受け、全コンピュータ停止。
- 3月14日、COVID-19向けワクチンの試験施設がランサムウェア「Maze」の攻撃を受け、個人情報窃取・同公開の被害。
- 3月22日、パリ周辺の大学病院等を統括するパリ公立病院連合（AP-HP）にDDoS攻撃。攻撃は1時間続き、この間、外部との接続が遮断。

（参考3）海外での混乱に乗じたフィッシングメール、偽アプリ、フェイクニュースなど

- 感染状況をトラッキングする偽アプリをダウンロードするとスマートフォンがロックされ、「ロック解除したければビットコインで100ドル払え」とのメッセージが表示。
- 新型コロナウイルスの感染状況をリアルタイムで確認できる米ジョンズ・ホプキンス大学HPを装った悪性ウェブサイトが多数出現。HPを閲覧しようとリンクをクリックするとマルウェアに感染し、個人情報が窃取。
- TV会議の招待メールに見せかけ、メール中のボタンを押すと、攻撃者Webサイトに誘導し、「会議はすでに始まっています」「あなたの参加を待機しています」など、焦らせるような文章が記載。
- 米軍所属の友人からの情報として「数日中にトランプ大統領が2週間の国家封鎖を実施する」とのテキストメッセージが急拡散。米NSCがツイッターでフェイクであると否定。

（本発表資料のお問い合わせ先）

〇近畿経済産業局 地域経済部
次世代産業・情報政策課長
大塚 公彦
担当者：中島、庄司
電　話：06－6966－6008
ＦＡＸ：06－6966－6097

〇近畿総合通信局
サイバーセキュリティ室／
電気通信事業課長　下村 英治
情報通信連携推進課長　中野 佳胤
担当者：和田、雲林院（うじい）
電　話：06－6942－8623
ＦＡＸ：06－6920－0609

令和２年４月 30 日
関西サイバーセキュリティ・ネットワーク事務局（近畿経済産業局、近畿総合通信局、一般財団法人関西情報センター））

テレワークを行う上での中小企業等の経営者の心構え５箇条

- 現在、新型コロナウイルスの感染拡大に伴って、在宅勤務やテレワークを実施する企業が増えていますが、この混乱に乗じて、サイバー攻撃、フィッシングメールや不正アプリ、フェイクニュースなどが増加しており、サイバーセキュリティ対策の必要性が高まっています。
- また、テレワークについては、新しいビジネスの創出や、時間・空間の有効活用につながり、多様化するライフスタイルの実現に寄与するものと考えられますので、今後においても重要な働き方のひとつです。
- テレワークを実施するうえで、次の心構え５箇条を意識するところから始めましょう。

1 社内での決まりを作って、ルールを守らせましょう

・テレワーク可能な業務、社内でのみ取り扱える業務の仕分けを行う責任者を決めましょう
・持ち帰ったデータは整理し、不要になったデータは削除しましょう
・社員が守るべき、守ることができる実効力のあるルールを明確にしましょう

2 責任者を決めて、技術情報を確認させましょう

・システム責任者を決め、必要な裁量、権限を与えましょう
・技術情報を収集させ、技術的に問題がないか確認させましょう
・自宅 PC を使う場合は、導入・制限するソフトウェアを確認しましょう

3 「社内ではない」という意識に切り替えましょう

・社内システムという城壁に守られた世界の外での業務を行う際の注意事項を確認しましょう
・持ち帰ったファイルや書類を整理し、クリアデスクを意識しましょう
（クリアデスク…離席する際に机の上に情報を記録したものを放置しないことを求める情報セキュリティの行動指針）
・「社内でない」という意識を持ち、家族・他人の目にも注意しましょう

4 積極的にコミュニケーションをとりましょう

・他の社員の目がないからこそコミュニケーションをとってお互いに注意喚起しましょう
・電話、Web 会議、チャット等を上手く活用し、意識を切り替える良いキッカケになる会話をしましょう
・何かあったときに迅速に対処できるよう、連絡方法を確認しておきましょう

5 人材を確保・育成しましょう

・困ったことがあれば、専門家（相談窓口）に相談しましょう
・人材が BCP（事業継続）の要、自社に必要なスキルを持ったコアになる人材を育てましょう
・働き方改革を推進するマネジメント人材を育てましょう

＜裏面には相談窓口、注意喚起、支援施策のサイト情報を掲載しています。＞

テレワーク、セキュリティに関する相談窓口や注意喚起、支援施策のサイトをご紹介します。詳細は各 HP をご覧ください。

テレワーク、セキュリティに関する相談窓口

○テレワークマネージャー相談窓口（総務省事業 ㈱NTT データ経営研究所へ事業委託）

Web 会議、電話にて、テレワークに適したシステムや情報セキュリティ、勤怠労務管理、その他テレワーク全般に関する情報提供・相談の窓口

https://www.nttdata-strategy.com/r01telework/

○テレワークに関する相談窓口（厚生労働省事業）

電話、メールにて、企業のテレワーク導入についての疑問・助成金手続きなどの相談窓口

https://telework.mhlw.go.jp/

○情報セキュリティ安心相談窓口（(独）情報処理推進機構）

メールにて、一般的な情報セキュリティ（主にウイルスや不正アクセス）に関する技術的な相談窓口

https://www.ipa.go.jp/security/anshin/index.html

テレワーク等に関する注意喚起

○テレワークを行う際のセキュリティ上の注意事項【令和 2 年 4 月 21 日】（(独）情報処理推進機構）

https://www.ipa.go.jp/security/announce/telework.html

○テレワークセキュリティガイドライン　第４版【令和 2 年 4 月 13 日】（総務省）

https://www.soumu.go.jp/main_content/000545372.pdf

○産業サイバーセキュリティ研究会による産業界に向けたメッセージ【令和 2 年 4 月 17 日】（経済産業省）

https://www.meti.go.jp/shingikai/mono_info_service/sangyo_cyber/pdf/20200417.pdf

○偽口座への送金を促す“ビジネスメール詐欺”の手口【令和 2 年 4 月 27 日】（(独)情報処理推進機構）

偽メールで国内企業が直接狙われる事例など、“ビジネスメール詐欺”の注意喚起サイト

https://www.ipa.go.jp/security/announce/2020-bec.html

新型コロナウイルス対策、テレワーク関連の支援施策情報

※令和２年度補正予算案の成立を前提としたものも含まれています。

○新型コロナウイルス感染症関連の施策一覧（経済産業省）

新型コロナウイルスの影響を受ける事業者に向けた支援策を掲載した総合サイトで、テレワーク導入に関する費用についての IT 導入補助金の「特別枠」、情報通信関連企業によるテレワークツールの提供等の支援プログラム、中小企業・小規模事業者を対象として経営上の相談窓口も掲載

https://www.meti.go.jp/covid-19/index.html

○新型コロナウイルス感染症対策としてのテレワークの活用について支援策を掲載した総合サイト（総務省）

テレワークお役立ち情報、テレワークにおけるセキュリティ確保、テレワークマネージャー相談窓口（上述）も掲載

https://www.soumu.go.jp/main_sosiki/joho_tsusin/telework/02ryutsu02_04000341.html

○働き方改革推進支援助成金【テレワークコース】（厚生労働省）

感染症の拡大防止対策として、テレワークを導入する場合に、機器・ソフト等の導入助成

https://www.mhlw.go.jp/stf/seisakunitsuite/bunya/koyou_roudou/roudoukijun/jikan/syokubaisikitelework.html

○地域 IoT 実装・共同利用推進事業（総務省）

地域の課題解決に資するサテライトオフィス等のテレワーク環境のモデル整備助成

https://www.soumu.go.jp/menu_news/s-news/01ryutsu06_02000246.html