JNSA 緊急事態宣言解除後の

セキュリティ・チェックリスト解説書

１．はじめに

新型コロナウイルス感染拡大によって、ICT を活用したテレワークが一気に一般化し、パラダイムシフトが実現しています。今までのテレワークは、事業活動におけるモバイルを前提とした職種向け、もしくは事業を継続する上で必要な非常時の仕組みとして整備をしている場合が主であったと考えます。しかしながら新型コロナ禍において、一気に通常業務の仕組みとして使用されるようになっています。セキュリティ管理を行う際の定石は、適用範囲の特定と例外事項の特定ですが、そのどちらもが実施しにくい状態なのが新型コロナ禍におけるテレワークの課題です。

一方、緊急措置的とはいえ一気にテレワークが拡大した状況は、With コロナ時代のニューノーマルさらには働き方改革の為の課題を解決する好機だと考えます。JNSA では、この緊急措置的なテレワークの利用からニューノーマルにおける新しい働き方を支える仕組みへ転換していく過程において、セキュリティの実効性を確保するための課題を抽出し、チェックリストとして作成しました。

２．チェックリストの活用方法

チェックリストでは、セキュリティの実効性を確保するために抽出した課題を大きく４つの観点にまとめています。これらは、緊急事態宣言解除を受けてテレワーク体制から通常の勤務体制に戻りつつある企業や組織のシステム管理担当者の方々に対応して頂きたい点を列挙しておりますので、本解説を参考に自組織における状況をご確認下さい。

なお、「３．緊急措置としてテレワークを許可した業務やルールを変更した業務の扱い」や「４．With コロナフェーズに向けた、業務見直しとセキュリティ対策」につきましては、システム管理者だけに限らず経営層の方々にもご一考頂きたい内容となっておりますので、是非この機会に、自組織の施策にお役立て下さい。

[1] 停止したシステムの再稼働における注意事項

(1) 長期間停止していたシステムの動作確認を行う

(2) 長期間停止していたシステム構成機器のセキュリティ対策の最新化を行う
（OS・ソフトウェアの最新化、アンチウイルスソフト定義ファイルの最新化等）

緊急事態宣言期間中、業務の縮退運用などにともないシステムを停止している場合があるかと思います。システムを再稼働する際は、問題なく稼働するか動作確認する必要があります。多くの組織が実施していると思いますが、まずシステム管理部門で動作確認をした後に、利用者に稼働開始を通知するようにしましょう。

また、稼働停止中に当該システムを構成する OS、ソフトウェアに対するアップデートが出ている可能性があります。セキュリティの基本中の基本であるソフトウェアの最新化を忘れずに行ってください。システム上で稼働するアンチウイルスソフトがある場合も、定義ファイルが最新になっているか確認してからシステムの利用開始をするようにしてください。たとえ、社内ネットワークにしか接続していないシステムであっても、社内ネットワークに侵入された後の踏み台になってしまう可能性もあるため、再稼働の後でも結構ですので、ソフトウェアを最新化する計画を立てるようにしましょう。ソフトウェアの脆弱性が明らかになっている場合には、暫定回避策（監視強化等）を合わせて実施することを推奨します。

[2] テレワークで社外に持ち出した機器を社内ネットワークに接続する際の注意事項

（1）持ち出した機器(端末や外部記憶媒体等)が紛失していないか棚卸し確認する

（2）端末のセキュリティ対策が最新化されているか確認する
（OS・ソフトウェアの最新化、アンチウイルスソフト定義ファイルの最新化等）

（3）持ち出した機器(端末や外部記憶媒体等)がマルウェアに感染していないか確認する

（4）無許可のソフトウェアがインストールされていないか確認する

今回の事態を受けて急遽テレワークを実施した組織は、特に端末の状況が把握しきれていないケースが多いと思います。情報資産の把握はセキュリティ上の基本であり、近年のセキュリティインシデントにおいても従業員の端末を通じて侵入される事例が多くありますので、この機会に全ての端末の利用状況を把握しましょう。この点を確認する具体的なチェックポイントがこれら４つの項目です。

資産管理ソフトや MDM（モバイル・デバイス・マネジメント）を導入している場合は中央管理されているため、確認することは比較的容易かと思います。そうでない場合は、システム担当者などが端末リストを元に、従業員に上記のチェック項目を確認することになるでしょう。従業員に確認させる場合は、「端末のセキュリティ対策の最新化」「マルウェア感染の有無」の確認方法まで示す必要があるかもしれません。（例えば Windows 10 の端末であれば、「Windows セキュリティ」の項目でグリーンのチェックマークがついているか等）

（5）テレワーク期間中に、社内システムに不正アクセスされていないかログ等を確認する

（6）社内ネットワークに接続した端末から不審な通信が行われていないか監視を一定期間強化する

前述の(1) ～ (4)を確認していることが前提となりますが、社内システムのログやネットワークログを取得している組織であれば、この期間のログをいつもより入念に確認することでセキュリティインシデントやインシデントにつながりうる問題がなかったかを確認することができます。そのためのチェックポイントがこれら２つの項目です。

テレワーク期間中は、普段とは違うシステムアクセスやネットワーク通信が発生していることも多いと思います。そういったものについて１つ１つ正規のアクセスであるか確認することが理想ですが、ログの分量によって難しいケースもあると思います。その場合でも、一部のログをランダムに抜粋して調査するなどは行った方が良いでしょう。この期間に他組織で発生したインシデント情報（セキュリティインテリジェンス）が JPCERT/CC や商用インテリジェンスサービスから入手できている場合には、そういった情報を元に自組織で類似の問題が起きていないかログを調査することも有効です。

[3] 緊急措置としてテレワークを許可した業務やルールを変更した業務の扱い

（1）緊急措置として許可した私物端末利用（BYOD）の利用実態について確認する
（私物端末のセキュリティ対策やマルウェア感染の有無、私物端末に保存されていた業務関連資料の削除確認等）

（2）緊急措置としてテレワークを許可していた業務やルールを変更した業務のリスクを再評価する

（3）再評価により、リスクが許容できると判断された業務については、引続きテレワークを継続すべく、必要に応じてセキュリティポリシー等の改訂を行うことを検討する

（4）再評価により、リスクが高いと判断された業務については、一旦元の運用に戻し、テレワークができる手段を検討したうえで、テレワークの可否を判断する

テレワーク・在宅勤務を前提としないかたちで OA 環境を運用していた組織では、新型コロナ禍における外出自粛要請を受けたテレワーク・在宅勤務化は、多くの場合、「緊急措置」あるいは「（ごく短い検討時間での）ルールやポリシー改定」を行うことで実施されたはずです。暫定的緊急処置として許可した、会社支給の PC 端末の持ち出し・持ち帰り、私物端末利用（BYOD）、業務データの保存と削除（どこに何を保管したか、また、それらの削除）、オンライン会議ツールのインストールなどは、勤務形態をオフィスに戻す場合・在宅を続行する場合の双方において、早期に棚卸しと確認が必要です。それらの確認結果を考慮したうえで、変更した（あるいは新規に策定した）ルールやポリシーにおけるリスクの洗い出しと再評価を実施し、特にテレワーク・在宅勤務を行うことでリスクが高いという分析結果になった業務については、一時的にもとの運用に戻しつつ、テレワークができる手段を検討してください。

With コロナ時代のニューノーマルにおいては、テレワーク・在宅勤務と在オフィス勤務の混在するハイブリッド勤務におけるセキュリティの担保を目指すことが求められます。

[4] With コロナフェーズに向けた、業務見直しとセキュリティ対策

ビジネスにおける With コロナ時代のニューノーマル対応で考慮しなくてはならないことは、常に新たな脅威との共存、すなわち「With コロナフェーズ」を考える必要があるということです。また、今後も新しいウイルスが出現する可能性や、近年の台風被害や発生が予想されている巨大地震など自然災害への備えも必要で、どうやって元の業務のやり方へ戻すのかを考えるのではなく、新しい業務のやり方を考えることが大切です。このため、ここでは、With コロナ時代のニューノーマルへ向けて企業・組織が中長期的に取組むべき項目を含めています。

(1) 第二波など緊急事態宣言の再要請に備え、業務移行の手順、必要なサービスを整理する

(2) テレワークにより負荷が集中した従業員や業務の洗い出しと対応の見直しを行う

(3) テレワークにより負荷が集中したサービスの洗い出しと対応の見直しを行う

(4) テレワークにより業務効率が下がった業務の洗い出しと対応の見直しを行う

(5) テレワークにできなかった業務の洗い出しと今後の対応について検討する

(6) 社内業務だけでなく、顧客や外部委託先との契約上、テレワーク化することができない業務やサービスについて、テレワークができる手段を検討し、顧客や外部委託先と協議の上、必要に応じて契約条件の見直しを検討する

まず、これら６項目ですが、一見するとなぜこれらがセキュリティ対策と関係するのか、という疑問を持たれる方がいるかもしれません。しかし企業・組織におけるセキュリティ対策の目的は、あくまで業務やビジネスを安心・安全に提供するためであり、セキュリティ対策だけを検討しても意味がありません。まずは、急に発令された緊急事態宣言下で実施してきた一時的なテレワークによる業務の状況について評価し、第二波への対応やその後の業務のやり方の恒久的な見直しについて検討を行う必要があります。「オフィスに行かないと仕事にならない。」「対面で話さないと営業効率が悪い。」と言った声がよく聞こえますが、本当にそうなのかについて冷静に評価し、対応を検討しましょう。対応を検討する際には、「全部オフィスを無くしたらどうなるか、無くすにはどういう条件がクリアされれば良いか」「全ての営業活動をオンラインにしたらどうなるか、オンライン営業を行うために必要な環境は？」という極端なケースを想定してみることで、新しいアイディアが出てくる場合があります。また、思い切って社内業務の一部をアウトソーシングしたらどうなるか、といった検討も有効です。さらに、多くの業務・ビジネスは自社・自組織に閉じて行われるわけではなく、顧客や外部委託先との関係がありますから、自社だけで検討するのではなく、様々なステークホルダーと協議することも忘れてはいけません。

（7）脱押印のためのオンラインワークフローや電子署名サービスの導入について検討する

（8）今までの IT 投資やセキュリティ対策の優先順位を見直し、テレワークを前提とした社内 IT 投資やセキュリティ対策について検討する

（9）テレワークを前提としたシステム構成管理やログ設定の見直しを行う

次にこれら３項目ですが、業務のやり方を見直す際に、IT をうまく活用しようという項目となります。「押印のためだけに出社した。」という笑えない話もあちらこちらで聞かれますが、日本のビジネスにおいて根強く残っている紙文書原本主義や押印文化について見直す絶好のタイミングであると捉えるべきです。また、今回の新型コロナ対応で一気に拡大した Web 会議ですが、社内 LAN やインターネット接続の帯域不足で音声や映像が途切れてしまうという事象も発生しています。テレワークを前提とした IT 投資やシステム構成について再検討が必要です。

（10）クラウドサービスや社内外で安全かつシームレスに業務を実施するためのゼロトラストネットワークの導入を推進する

（11）テレワークを前提としたセキュリティインシデント発生時の体制や対応について再検討を行うと共に、そのための教育や訓練を行う

（12）これを機会に、リスクの再評価を行い、セキュリティポリシーにおいて形骸化した項目を見直すと共に、社員等への周知やセキュリティリテラシーの向上を行う

さらにこれら３項目は、新しい業務のやり方において検討すべきセキュリティに関連した項目となります。テレワークを前提とした IT システムではリモートアクセスやクラウドサービスの活用が効率化に必須となりますが、その場合、今までのように社内を安全に保ち、社外からの侵入を重点的に防ぐという境界防御型のセキュリティの考え方が通用しなくなってきています。この機会に、「全て信頼できない（ゼロトラスト）」という前提で、全てのユーザ、デバイス、場所、セッションのリスクを評価し、動的なアクセス制御を行うゼロトラストネットワークの導入について検討することを推奨します。また、多くの企業・組織において意外と考慮されていないのは、セキュリティポリシーやセキュリティインシデント対応がテレワークを想定していなかったという点です。これを機会に見直しを行うと共に、見直しを実施した項目について、社員への教育、訓練を行うことも忘れないようにしましょう。

３．一般従業員がチェックすべき事項

ここまで説明してきたチェックリストは、主に情報システムや組織の管理者向けのものとなっていますが、ここからは、自宅に会社パソコンなどの機材を持ちだしテレワークをしていた一般の従業員の方が、緊急事態宣言が解除されたことで、久しぶりにオフィスに会社パソコンを持ち帰って仕事を開始する時に気を付けるべき項目について解説します。ポイントは正直にありのままの状況を会社や上司と共有するということです。隠していて後で発覚した場合、自身の責任を問われるだけでなく、会社の被害も増大させる可能性があります。

（1）会社のネットワークにつなぐ前に、セキュリティ対策を最新にすること

（2）持ち出した機器を紛失・破損をしてしまったら、正直に報告すること

（3）在宅勤務中に無断でインストールしたソフトがあれば、全て報告すること

（4）在宅勤務中に、怪しい動きなどの心配なことがあったら、すぐに報告すること

（5）在宅勤務中に私物パソコンを使って業務を行った場合には、その事実を報告すること

（6）在宅に必要な機器を整理し、ハイブリット勤務に備えること

（7）在宅でもできる仕事、在宅ではリスクがある仕事をリストアップして業務を見直すこと

（8）会社のセキュリティルールに課題があれば、リストアップして報告すること

(1) 会社のネットワークにつなぐ前に、セキュリティ対策を最新にすること

４月の頭から在宅勤務が始まり１か月以上、会社のネットワークに直接接続していないパソコンは、会社のネットワークにつなぐ前に、自宅で最新パッチを適用し、全ての記憶領域のウイルススキャンをしてから、会社に持ち込みましょう。もちろん、スキャン前にアンチウイルスソフトの定義ファイルを最新化することも忘れないでください。

(2) 持ち出した機器を紛失・破損をしてしまったら、正直に報告すること

自宅での勤務では、飲み物や食べ物がオフィスよりも自由になります。飲み物などを、キーボードやマウスにこぼして、壊してしまった場合には、正直に申告して修理や代替品の手配をお願いしましょう。

(3) 在宅勤務中に無断でインストールしたソフトがあれば、全て報告すること

取引先や連携企業の要望により、Webex、Teams、Zoom などの Web 会議ツールや、Slack などのコミュニケーションツールを急遽インストールしたのではないでしょうか。それらが、会社として許可されていない場合には、インストールしたツールを全て上司や情報システム部門に報告しましょう。継続して利用したい場合は、会社のルールに従った対応をしましょう。

(4) 在宅勤務中に、怪しい動きなどの心配なことがあったら、すぐに報告すること

自宅のネットワーク環境は、オフィス内に比べセキュリティレベルが低い状態であることが多いと思います。自宅でインターネットを閲覧している最中や、メールを開いたときに、怪しい動きだと感じたら、躊躇せず、上司や情報システム部門にすぐに報告しましょう。

(5) 在宅勤務中に私物パソコンを使って業務を行った場合には、その事実を報告すること

やむを得ず会社支給のパソコンや USB メモリではなく私物パソコン等を業務に使っていませんか。私物パソコンは一般的にセキュリティ対策が弱いと考えられます。やむを得ず使ってしまった場合でも、業務に関連する情報は削除した上で、上司や情報システム部門に報告しましょう。

(6) 在宅に必要な機器を整理し、ハイブリット勤務に備えること

パソコンや電源ケーブル、モニタなどを一時的に会社から持ち出した場合や自費で購入したものがあると思います。生産性を落とさない働き方のために、会社と自宅の両方に据え付けておくべきものや、会社と自宅で持ち運びすべきものを整理しましょう。自費購入したものを業務で利用する場合のルールや場合によっては経費精算が可能かどうかも確認しておきましょう。

(7) 在宅でもできる仕事、在宅ではリスクがある仕事をリストアップして業務を見直すこと

緊急措置としてテレワークに移行したことで、出社しなくてもできる仕事が沢山ある事に気が付くことができたはずですが、逆に社外で行うにはリスクが伴う仕事も明らかになっているはずです。これらを整理して、働き方の見直し、さらには事業の見直しのため、会社や上司と情報共有しましょう。

(8) 会社のセキュリティルールに課題があれば、リストアップして報告すること

今回の在宅勤務で、当たり前に行われていたセキュリティのルールにある矛盾や不都合に気が付いたのではないでしょうか。いい機会ですから、セキュリティルールの見直し、テレワークによる生産性向上のための改善提案に活かしましょう。

４．企業へのアドバイス

「テレワーク先でもオフィスとまったく同じように業務ができる」ことを目指そうとすると、快適な業務環境を確保するために必要なネットワーク設備やセキュリティ対策がそれなりに大掛かりになり、コストもかかります。たとえば、テレワーク先で機密情報を用いた作業ができるようとする場合、その保護のためにテレワークに用いる端末に機密情報を保存するのではなく、安全な環境にある端末をテレワーク環境からあたかも遠隔操作するように扱う方法（リモートデスクトップやシンクライアント方式などと呼ばれます）を用いるのが一般的です。しかしながらこの方法で快適に作業するには高速のネットワーク回線が欠かせません。一方、テレワーク環境では機密情報を扱わないことにすれば、職場で用いているノートパソコンを持ち帰ってもらい、暗号化された通信でオフィスや他の従業員とやりとりするような方法でもよく、その場合ネットワークは遅めでもなんとかなります。このように、テレワークを行うときに「必ずこうしなければならない」という決まった方法があるわけではないので、テレワークで行いたい業務の内容や、扱う情報の特徴に応じて最も適した方法を選ぶことが重要です。

また、セキュリティビジネスを営む企業を主たる会員とする JNSA が書くと営業トークと受け取られてしまうかもしれませんが、セキュリティ人材が必ずしも潤沢でない企業においては、自社でやらねばならない対策とプロにアウトソースできる対策を明確にし、限られたリソースを効果的・効率的に使用することが重要です。昨今の報道にもあるとおり、大手の電機メーカーもサイバー攻撃の被害を受けてしまうような状況の中、自社サーバーへのアクセスログのうち、どれがテレワークからのアクセスで、どれがサイバー攻撃なのかを正しく区別するのは容易ではありません。最近は中小企業向けの SOC（セキュリティオペレーションセンター）サービスのように、規模の小さな企業にとっても利用しやすいサービスが増えています。経済産業省と独立行政法人情報処理推進機構（IPA）ではこうした動きを支援するため、一定の品質を満たすサービスを「情報セキュリティサービス基準適合サービスリスト」(*1)に掲載して公表しています。また、JNSA でも会員企業が提供するセキュリティ製品やサービスを「JNSA ソリューションガイド」(*2)として公表していますので、参考にしていただければと思います。

(*1) https://www.ipa.go.jp/security/it-service/service_list.html
(*2) https://www.jnsa.org/JNSASolutionGuide/IndexAction.do