NTT 東日本 - IPA 「シン・テレワークシステム」向け

セキュリティポリシー

2020 年 4 月 30 日 Ver.0.14 Beta 4 対応

（ワンタイムパスワード、パスワード複雑性対応）

Ver.1.12

2020 年 5 月 14 日
一般社団法人コンピュータソフトウェア協会

1　はじめに

新型コロナウイルス感染症による緊急事態宣言により、接触機会の 8 割削減が強く求められる中、在宅勤務の重要性が増しています。
一方で、多くの企業は在宅勤務を前提とした情報システムを構築していません。また、多くの中小企業は VPN 環境を保有しておらず、業務遂行のためにやむなく通勤を強いられている状況にあります。こうした中で、NTT 東日本と IPA は誰でも簡単に利用できるリモートデスクトップ型のテレワークシステム「シン・テレワークシステム」を緊急構築し、本年 4 月 21 日から実証実験として無償で提供を開始しました。「シン・テレワークシステム」は企業内の PC にサーバーソフトをインストールし、在宅の PC にクライアントソフトをインストールすることで、暗号化された VPN 環境を提供するもので、在宅 PC からリモートデスクトップ接続することで、企業内 PC を操作することが可能です。
他方、在宅 PC から企業 PC に接続する際のセキュリティがしっかりと担保されることが重要です。
本書は「シン・テレワークシステム」が安心・安全に運用されるためのセキュリティ設定を、当協会有志が急遽取りまとめたものです。セキュリティが担保された「シン・テレワークシステム」で在宅勤務が推進され、国民全体でコロナ禍に打ち勝つことを祈念しております。

2020 年 4 月 28 日

一般社団法人コンピュータソフトウェア協会
セキュリティ委員会
Software ISAC

企業における運用上の過不足などのご指摘をお待ちしております。改版の際は、当協会のホームページ及び Software ISAC ホームページでお知らせいたします。

2 シン・テレワークシステムのセキュリティポリシーの概要

2.1 背景と要求事項

コロナ禍における接触機会 80%減を実現するためには在宅勤務が極めて有効です。一方で、中小企業での在宅勤務の実現には以下の課題があると考えられます。

- ✓ 多くの在宅業務では企業ネットワークと VPN 接続が必要
- ✓ 宅内ネットワークのセキュリティ状況やネットワークへの接続状況が一律でない
- ✓ 個人情報や営業情報、状況に応じ機密情報を取り扱うケースがあり得る
- ✓ リスク回避のための新たな設備投資や運用負担の増加が見込まれる
- ✓ 新たな就業規則や運用規程の策定や従業員教育が必要となる

売上が急減し新たな設備投資が難しい状況にある中で、「シン・テレワークシステム」は有効なソリューションとなりますが、企業ネットワークのセグメントが社員の自宅まで延長されるよるリスク分析や懸念事項の解消は、経営者やシステム管理者にとって非常に大きな負担と言わざるを得ません。

こうした懸念や負担を軽減し、利用者にセキュリティ意識を高めることが本ポリシーに要求されるものです。

2.2 本ポリシー策定における基本的な考え方

策定にあたっては、様々な在宅勤務の様態がありリスクが大きく異なることから、次のような考え方をとりました。

- ✓ 企業規模に関わらず汎用的に使用できるものを目指し、かつ、在宅勤務を検討する際の「気づき」となるように構成する
- ✓ 成果物の改変を自由に、また容易にする
- ✓ ISMS、P マーク、情報安全確保支援士等の資格取得を前提としない
- ✓ 「シン・テレワークシステム」を前提としてシステムのスコープを絞るが、異なるシステムでも読み替えが容易であること
- ✓ 在宅側のセキュリティ項目（課題）を具体的に網羅するとともに、自己分析が可能なツールを用意する
- ✓ 利用者のセキュリティレベルの底上げを図り、企業のセキュリティ向上に資するものとする

2.3 本ポリシーのスコープ

前述のように、在宅勤務には、様々な形態が考えられることから、本ポリシーは、以下をスコープおよび前提条件として策定されています。

- ■ 対象企業： 国内の大半をなす 50 名以下の中小企業
- ■ 対象ユーザー： 対象企業の従業員、役員とし、セキュリティ知識を有しない
- ■ 業務内容： 完全性、機密性の確保が求められる業務
- ■ 端末： 在宅の個人保有の Windows PC

- 宅内 LAN 環境： 有線もしくは無線 LAN を利用し、エッジルーターには一般的な家庭用ルーターを利用し、ISP を通じてインターネット回線に接続している
  もしくは、スマートフォンによるテザリングの利用
- 企業 LAN 環境： 企業側のネットワークには Firewall もしくはルーターが設置
  Active Directory もしくは Work Group が構成

本ポリシーのスコープには、以下が含まれないことに注意し、個別に対応してください。

- 個人情報、センシティブな情報の保護のためには、個別のリスクに応じて必要とされる機能や役割、就業規則に関連する規程の追加が必要です。これらの保護を保証するものではありません。
- 可用性の確保や、否認防止、責任追及性を保証するものではありません。

2.4 テーラリング

本ポリシーは事業状況、利用状況に応じて、テーラリング (tailoring) できるものとします。不足している機能を追加したり、過剰と思われる項目を削除したり、現状の業務にあわせて改変することは自由です。リスク分析に基づいたテーラリングを推奨します。

2.5 システム構成に対する基本的な考え方

シン・テレワークシステム： Windows 版共有機能無効版サーバー
対象 OS： Windows 8.1, 10, Windows Server 2012, 2016, 2019 (R2 含む)
※サポートが終了した OS での運用は極めて危険であり、第三者にセキュリティ的な被害を提供する恐れもあります。サポートが終了した OS での運用は、ウイルス感染、なりすまし、乗っ取り、情報漏洩、踏み台による第三者への攻撃などのリスクを受容していることを正確に認識した上で、利用を極力控え、早急にシステムの切り替えを頂くよう強く要請します。

2.6 遵守事項、推奨事項、許容事項について

ポリシーは想定状況や事例に応じて、遵守事項 (SHALL:するものとする、SHALL NOT：しないものとする) と、推奨事項 (SHOULD：すべきである、SHOULD NOT：すべきではない) 、許容事項（MAY:してもよい、NEED NOT：しなくてもよい）を記述していますが、あくまでも目安であり、利用者のリスクに応じた整合性が確保されるとは限らないことに留意してください

2.7 ポリシー分類

ポリシーは以下の分類を策定しています。

- 宅内 PC、宅内ネットワーク、企業内 PC に設定するシン・テレワークシステム
- 企業内 Active Directory（管理者向け）

また、在宅勤務のセキュリティ規程例については、企業の就業規則や既存の規程との整合性は保証されないため、適用にあたっては十分留意してください。

3 シン・テレワークシステムのセキュリティポリシー

3.1 在宅 PC への要求事項

在宅 PC は以下の要求を満たして下さい。

3.1.1 在宅 PC のデータ管理

必要なデータの管理：

業務に必要なデータや情報を在宅PCにコピーしない、保存しないこと

リモートデスクトップ機能のクリップボードのリダイレクト、ディスクやプリンターのリダイレクトは利用しないでください。企業PCから在宅PCへのデータのコピーや、ディスクの共有などの行為は、情報漏洩の原因になるため、必ず、企業PC内で処理が完結するようにしてください。（遵守事項）

業務に必要なデータや情報を在宅PCにコピーする場合

業務の性質上、在宅PCにデータをコピーせざるを得ない場合は、対象となる業務と在宅PCにコピーするファイルを特定し文書化した上で、許可するようにして下さい。在宅PCに保存されるファイルは必ず暗号化し、情報漏洩対策を講じてください。（遵守事項）

3.1.2 在宅 PC の脆弱性管理

OS、ミドルウェア、アプリケーションの脆弱性管理：

OS、デスクトップアプリケーションソフト、クラウドシステム、使用するブラウザ、java、Flash等、搭載されているすべてのソフトウェアの脆弱性修正プログラムの適用状況を把握すること

在宅PCは常に最新の状態であることが求められます。ソフトウェアのアップデートを確認し、修正プログラムは必ず適用してください。（遵守事項）

3.1.3 在宅 PC のアンチウイルスソフトによる完全スキャン

在宅PCのアンチウイルスソフト完全スキャン：

マルウェアに感染した時点でアンチウイルスソフトが未対応であり、マルウェア感染が見過ごされることを防ぐこと

週に1回以上、アンチウイルスソフトのパターンファイルを最新に更新したうえで、在宅PCに接続されているすべてのドライブの完全スキャンを実施してください。（遵守事項）

管理者は、完全スキャンの自動スケジューリング、実施状況やマルウェアの検出状況を把握してください。（推奨事項）

新たなマルウェアが発生した時点で、アンチウイルスソフトウェアがそのハッシュ値やふるまい、特徴を把握しておらず、マルウェアとして認識せずに見逃してしまうことがあります。一方で、独自の情報収集や利用者からの報告によって、マルウェアを認識するように日々パターンファイルや認識メカニズムは更新されている（この間はマルウェアが潜伏しているdeltaとなります）。そこで、見逃した潜伏しているマルウェアを検出するには、すべてのファイルをスキャンする完全スキャンが必要です。他方、完全スキャンには時間がかかることが多く、その間、PCの動作が重くなることから、休日に実施してください。

3.1.4　在宅 PC のアンチウイルスソフトによる電子メールの検知

在宅PCのアンチウイルスソフトの電子メール検知：
電子メールからのマルウェアの感染を防ぐこと
マルウェアの感染源として、もっとも多いとされるのは、電子メールの添付ファイルや埋め込まれたリンクと言われています。電子メールのアンチウイルスソフトによるマルウェア検出を設定してください。（遵守事項）
管理者は、電子メールのマルウェア検出設定や検出状況を把握してください。（推奨事項）

マルウェアの大半は電子メールを利用して感染を拡大します。多くのアンチウイルスソフトウェアは電子メールの添付ファイルに潜むマルウェアを検出できるようになっていますが、必ずしも既定の設定で電子メールのマルウェア検出を行うとは限りません。また、ユーザーが故意もしくは誤って設定を変更してしまっている可能性もあるので、設定状況を把握することは重要です。

3.1.5　パスワード漏洩のチェック

在宅PC、企業PCで使用しているパスワードの漏洩検知：
漏洩したパスワードでの不正侵入、乗っ取りを防ぐこと
インターネット上でサービスを提供するベンダーには、ユーザーのパスワードが保存されていますが、ベンダーがサイバー攻撃にあい大量のユーザーデータ（電子メールアドレス、ID、パスワードなど）が漏洩した事件が多数あります。攻撃者はこれらの電子メールアドレスやパスワードを使って侵入を試みます。どのように長くて複雑なパスワードでも漏洩してしまえば、侵入を許すことになります。自分の電子メールアドレスやパスワードの漏洩をチェックできる海外サイトがありますので、チェックをして下さい。（推奨事項）

https://haveibeenpwned.com/
電子メールアドレスを入力するだけで漏洩の判定ができます。

3.2 宅内ネットワークへの要求事項

宅内ネットワークは以下の要求を満たしてください。

3.2.1　無線 LAN のプロトコル

宅内ネットワークで無線LANを使用する際は、Wi-Fiのセキュリティ規格であるWPA2もしくはWPA3を使用する：
脆弱な無線LANプロトコルの使用による情報漏洩を防ぐこと
無線LANの接続にはWPA2もしくは最新のWPA3を使用し、暗号化はAESを選択して下さい。WPAの事前共有鍵は、手動でパスフレーズを設定する場合は20桁以上(（IEEE 802.11推奨値)として下さい。極力、無線LANルーターに付属する事前共有鍵の自動設定機能(Wi-Fi Protected Setup)を使用しましょう。また、WPA2、WPA3には脆弱性が指摘されているため、無線LANルーターのファームウェアアップデートを、マニュアルやコールセンターの指示のもと確認して実施してください。また、古いセキュリティ規格であるWEPは使用しないでください。簡単に暗号化したデータが解読されてしまいます。（遵守事項）

3.2.2　宅内ネットワークのルーターのパケットフィルタ

宅内ネットワークのエッジルーターは、初期設定パスワードを変更し、パケットフィルタを設定する：
インターネット側からの攻撃や不正侵入を防ぐこと
ADSLや光回線に接続するためのルーターの初期設定の管理者パスワードをなるべく長い桁数（16桁以上、設定できない場合は最大値）に変更して下さい。下表の送信元ポート（WAN→LAN）の通信廃棄（拒否）設定をして下さい。変更したパスワードは手帳やノートに記録しましょう。（遵守事項）

設定方法が不明な場合は、メーカーのサポートセンターに「WANからLANあての通信の破棄（拒否）設定をしたい」といって相談しましょう。また、ランサムウェアなどの被害にあわないように適切な外部通信設定がなされているかを、無償で診断できるサイトがありますので、確認ください。
株式会社ラック（東京証券取引所JASDAQ上場）提供 「自診くん」 https://jisin.lac.co.jp/

WAN → LAN 破棄（拒否）するポート	説明
20/TCP・UDP	ftp data
21/TCP・UDP	ftp
23/TCP・UDP	telnet
135/TCP・UDP	DCE/RPC
137/TCP・UDP	NetBIOS Name Service
138/TCP・UDP	NetBIOS Datagram Service
139/TCP・UDP	NetBIOS Session Service
445/TCP・UDP	Microsoft-DS SMB file sharing
2049/TCP・UDP	NFS
5900/TCP	VNC

3.3 企業内 PC に設定するシン・テレワークシステムへの要求事項

3.3.1　共有機能無効版の使用

ダウンロードモジュールはWindows版共有機能無効版サーバーを選択する：
共有機能は無効にしてリモートPCからの情報漏洩を防ぐこと
企業PCから宅内PCへのファイルのコピーなどを防ぎ、情報が企業内から流出しないように設定して下さい。フルパッケージ版をダウンロードした場合は、動作設定で[共有機能の使用を禁止する] を有効にしてください。
但し、印刷などを宅内PCで実施する必要があるなどの場合は、共有機能を利用し、ファイルの管理に十分留意してフルパッケージ版を利用してください。(推奨事項)

業務の都合上、共有機能を許可する場合は、業務内容、共有するファイルを特定し、取り扱い規程を定めて運用してください。参照：4.3 シン・テレワークシステムを利用して企業PCに宅内PCから接続する場合

3.3.2 [パスワードのみによる簡易ユーザー認証]の設定

[パスワード認証を使用して、このコンピュータを安全にする]を設定する際は、長いパスフレーズを設定する：

16桁以上の複雑なパスワードか、24桁以上の複雑でない長いパスフレーズを設定し本人以外の接続を防ぐこと

第三者が推測しやすいパスワードは使用しないでください。“P@ssw0rd” などの安直な設定は絶対に避けてください。また、大文字、小文字、数字、記号を有する複雑なパスワードであっても、コンピュータの計算能力が向上した現在では、8桁では十分な強度を有するとは言えません。

◆16桁以上の複雑なパスワードの場合

16 桁以上で、小文字・大文字・数字・記号のうち少なくとも 2 種類以上を使用してください。

◆24桁以上の複雑でないパスワードの場合

設定するパスワードはなるべく長いパスフレーズを設定して下さい。記号や数値を必ず入れる必要はありません。

hayaku_corona_ga_nakunarimasuyouni!　　35桁

iryoukikann-no-minasan-arigatougozaimsu　39桁　(推奨事項)

※上記はあくまでも例示です。記載のパスワードをそのままコピーして使用しないでください。

宅内PCを家族で共有している場合に、家族が企業PCに接続したりすることのないように、宅内PCのログオンパスワードなどの使いまわしは、絶対に避けてください。また、2020年4月27日 Ver.0.13 Beta3 からパスワードのポリシーが変更されたのに対応しました。

3.3.3 [ワンタイムパスワード認証(OTP)]の使用

[ワンタイムパスワード認証(OTP)]を使用する：

多要素認証で第三者の接続を防ぐこと

ログイン時に事前設定したメールアドレスにワンタイムパスワード（OTP）を送信することで、事前設定したパスフレーズと、メールに着信した5分間有効な一度限りのOTPで、第三者のなりすましを防ぐことができ、安全性が飛躍的に高まります。本機能は、セキュリティ確保に極めて有効なものですので、必ず設定して下さい。

2020年4月30日 Ver.0.14 Beta4 からワンタイムパスワード機能が追加されたことに対応しました。

3.3.4 [高度なユーザー認証機能を使用する]の設定

[NT ドメイン認証]、[RADIUS認証]を設定する際は、ユーザー名に ‘*’(アスタリスク) を使用しない：

本人以外の接続を防ぐこと

ユーザー名に ‘*’ (アスタリスク)を入力すると、NT ドメインユーザーもしくはRADIUSサーバーに登録されたユーザーがログオン可能となり、本人以外のユーザーが接続可能となるため、ユーザー名は必ず本人のIDを登録して下さい。（遵守事項）

3.3.5 [通信の暗号化と盗聴・改ざんの防止]の設定

[TLS プロトコルにおける証明書の検証を有効にする] を有効にする：
盗聴・改ざんを防ぐこと
通信経路上の盗聴や改ざんを防止するため、必ずチェックボックスにチェックを入れてください。プロキシサーバーやファイアウォールを経由した場合にエラーが発生する場合は、シン・テレワークシステム以外の接続方法を検討して下さい。（遵守事項）

3.4 企業内 Active Directory（情報システム管理者向け）

企業内に Windows Active Directory が設定されている場合は、以下の要求を満たしてください。Active Directory ではなく、Workgroup の場合は無視して下さい。

3.4.1 グループポリシー

リモートデスクトップのグループポリシーを設定する：
通信経路の暗号化を行うとともにリモートデスクトップ経由の情報転送を防ぐこと
利用者が共有機能を許可にしても、グループポリシーで共有機能を禁止に設定可能です。業務内容、企業のセキュリティポリシーに従って、適宜、設定して下さい。なお、グループポリシーを変更後は、コマンドプロンプトからGPUPDATE /FORCE の実行し、セッションをいったん切って、再接続する必要があります。（遵守事項）

グループポリシー			値	オプション	値
[コンピュータの構成]> [ポリシー]> [管理用テンプレート]> [Windows コンポーネント]> [リモート デスクトップ サービス]>	[セキュリティ]>	[クライアント接続の暗号化レベルを設定する]	有効	暗号化レベル	高レベル
		[接続するたびにパスワードを要求する]	有効		
		[セキュリティで保護された RPC 通信を要求する]	有効		
		[ローカルの管理者によるアクセス許可のカスタマイズを許可しない]	有効		
	[セッションの時間制限]>	[アクティブでアイドル状態になっているリモートデスクトップサービス セッションの制限時間を設定する]	有効	アイドルセッションの制限	30 分
	[デバイスとリソースのリダイレクト]>	[クリップボードのリダイレクトを許可しない]	有効		
		[COM ポートのリダイレクトを許可しない]	有効		
		[ドライブのリダイレクトを許可しない]	有効		
	[プリンターのリダイレクト]>	[LPT ポートのリダイレクトを許可しない]	有効		
		[クライアントの通常使うプリンターをセッションで通常使うプリンターに設定しない]	有効		
	[リモート デスクトップ接続のクライアント]>	[クライアント プリンターのリダイレクトを許可しない]	有効		
		[クライアント プリンターのリダイレクトを許可しない]	有効		
		[パスワードの保存を許可しない]	有効		

3.4.2 ドメインで使用可能なプロトコル

ドメインコントローラー、サーバー、ワークステーションでは脆弱なプロトコルをグループポリシーで禁止設定する：
Windowsの古いプロトコルの脆弱性を利用するマルウェア等の被害を防ぐため、後方互換性に配慮しつつ、Lan Manager、NTLMv1、SMBv1を禁止する。（遵守事項）
古いプロトコルしか利用できないNAS等の調査を実施し、撤廃、リプレースを行う。（遵守事項）
NTLMの監査を実施する。（推奨事項）

マイクロソフトが使用を推奨していないプロトコルの脆弱性を利用するマルウェア、特にランサムウェアの被害が増加したことを踏まえ、Lan Manager、NTLMv1、SMBv1を禁止してください。なお、古いNASなどでこれらのプロトコルが必要なものは、早急にリプレースを計画して下さい。

3.4.3 ドメインアカウントポリシー

ドメインのアカウントポリシーを設定し、全社的にパスワードの最低長、アカウントロックを強制設定する：
ブルートフォース攻撃や辞書攻撃等での不正侵入、乗っ取りを防ぐこと
Active Directoryのドメイン グループポリシーでアカウントロックアウトのポリシーを設定して下さい。アカウントロックアウトの閾値を10回ログオンに失敗ロックアウト期間を30分に設定します。（遵守事項）
複雑性を求めない長いパスフレーズの使用もしくはWindows helloによる多要素認証を検討してください。（推奨事項）

4　在宅勤務におけるセキュリティ規程

在宅勤務に関わる規程は、以下の要件を満たすようにしてください。すべての規程は実効性を担保するため、従業員への詳しい説明と違反の際の懲罰規程を設けることが必要です。

4.1 データの暗号化

個人情報や企業情報が含まれるデータファイルには、必ずパスワードを設定し、暗号化する規程を設ける。電子メールの添付ファイルとして暗号化データを送信する場合、復号用のパスワードを電子メール（平文）で送信しないように規程することが望まれます。

規程例：

第〇条（データの暗号化）

1．個人情報や営業情報が含まれるデータファイルは、会社規程の暗号化方式で暗号化しなければならない。暗号化のためのパスワードは、以下のいずれかの特性を有し、第三者から推測困難なければならない。

a. 16 桁以上の長さで、かつ、大文字、小文字、数字、記号のうち 2 種類以上が使用されている。

b. 24 桁以上である。

パスワードの受け渡しに電子メールを利用してはならない。

2．データファイルとパスワードを収めた電子ファイルは必ず格納する媒体単位で分離して保管し、同一の記録媒体、サーバー、端末に保管してはならない。

第〇条（暗号化方式）

1．当社の暗号化方式は以下のとおりとする。

データ暗号：　　AES ブロック長 256 ビット、鍵長 256bit

メッセージダイジェスト：　SHA-256

セキュリティ通信：　　TLS1.2 以上

2．但し、顧客都合、システム都合で当社規程を充足できない場合は、想定されるリスクと対策を文書でシステム管理部門に申請し、個別に許可を受けることで使用できる。

4.2 認証情報の保全

ID、パスワードなどのユーザー認証に使用される認証情報（クレデンシャル）は、電子メールを使用せず、相手が特定できる経路で通知、連絡して下さい。

規程例：

第〇条（認証情報の連絡方法）

1．ユーザー認証に使用される ID、パスワードは、社内、社外を問わず電子メール、USB メモリを使って相手方に受け渡しをしてはならない。

2．認証情報が記録された紙媒体は、必ず、鍵のかかるロッカー等に保管しなければならない。

3．相手方への認証情報の受け渡し方法として以下の方法を利用する。

A）紙媒体の場合は、簡易書留で送付する事とし、電話、電子メール等で事前に相手方に通知を行っておく。この場合、認証情報一式（ID と PW などの認証情報）を送付してもよい。
B）電話の場合は、当方から相手方に電話をかけたうえで本人であることを確認する。この場合、認証情報一式を口頭で伝達してもよい。
C）FAX の場合は、受け取り相手が受信用紙を直接受け取れる状態を確認した上で送信する。誤送信に備え、認証情報一式を送付してはならない。必ず、パスワードは単独で送信する。
D）携帯電話のショートメッセージの場合は、事前に相手方に送付通知を行っておく。誤送信に備え、認証情報一式を送付してはならない。必ず、パスワードは単独で送信する。
E）クラウドストレージの場合は、クラウドストレージへのログオンのための認証所法を前項 A から D の方法で受け渡した場合に限り、当該認証情報一式を送付してもよい。但し、相手方が認証情報一式を受領した後、速やかに削除しなければならない。
4．前項 C および D で誤送信が判明した場合は、該当するシステムから誤送信した認証情報をすべて破棄し、当社管理者に届けなければならない。

4.3 シン・テレワークシステムを利用して企業 PC に宅内 PC から接続する場合

企業が定めたセキュリティポリシーの遵守が求められるため、ポリシーに合致する規程の整備が必要です。

規定例：
第〇条（シン・テレワークシステムの利用）
1．会社の許可なく、シン・テレワークシステムを企業 PC にインストールし、もしくは使用をしてはならない。
2．シン・テレワークシステムを利用する場合は、別途定めたシン・テレワークシステムセキュリティポリシーを遵守しなければならない。
3．在宅 PC がウイルスに感染した場合、もしくは操作ミス等で情報漏洩等が疑われる場合は、状況を速やかに会社に報告し、会社の指示に従わなければならない。
4．在宅勤務が不要となった場合は、シン・テレワークシステムをアンインストールしなければならない。

第〇条（シン・テレワークシステムの共有機能の利用）
1．会社の許可なく、在宅 PC と企業 PC 間でファイル、ドライブ、プリンターの共有を行ってはならない。
2．業務の遂行上、共有機能が必要な場合は、会社に届け出をし、承認を受けなければならない。
3．在宅 PC で会社のファイルの閲覧、変更を行い、企業 PC にファイルを戻す場合は、ウイルス感染を防ぐために、私的なインターネットの閲覧やメールを行ってはならない。
4．在宅 PC で業務上の印刷を行う場合は必要最低限とする。不要となった印刷物は情報漏洩を避けるため、シュレッダーで裁断し廃棄するか、会社に送付して処分しなければならない。

第〇条（在宅 PC のアンチウイルスソフト）
1．在宅 PC には、必ず、最新のアンチウイルスソフトを稼働させなければならない。

2. 在宅 PC のアンチウイルスソフトは、日次 1 回以上のクィックスキャンを実行し、週次 1 回以上の完全スキャンを実施しなければならない。万一、ウイルス感染が発見された場合は、シン・テレワークシステムの利用を即座に停止し、速やかに会社に報告した上で指示を仰がなくてはならない。

第〇条（シン・テレワークシステムの認証情報）

1. シン・テレワークシステムの認証情報は、以下のいずれかの特性を有し、第三者から推測困難なければならない。
    a. 16 桁以上の長さで、かつ、大文字、小文字、数字、記号のうち 2 種類以上が使用されている。
    b. 24 桁以上である。
2. シン・テレワークシステムの認証情報は、シン・テレワークシステム専用とし、他のシステムや Web サイト等で使用してはならない。
3. シン・テレワークシステムはワンタイムパスワードを必ず使用しなければならない。

以上

Ver.1 2020 年 4 月 28 日公表
Ver.1.1 2020 年 5 月 1 日公表
Ver1.12 2020 年 5 月 14 日公表

一般社団法人コンピュータソフトウェア協会
〒107-0052 東京都港区赤坂 1-3-6　赤坂グレースビル
TEL：03-3560-8440／FAX：03-3560-8441
https://csaj.jp

継承 ー もしあなたがこの資料をリミックスしたり、改変したり、加工した場合には、あなたはあなたの貢献部分を元の作品と同じライセンスの下に頒布しなければなりません。
追加的な制約は課せません ー あなたは、このライセンスが他の者に許諾することを法的に制限するようないかなる法的規定も技術的手段 も適用してはなりません。