4.オフィス内業務のＤＸ（デジタルトランスフォーメーション）

Point

・「業務を切り分ける」テレワークは非効率
・普段の仕事をデジタル化すればテレワークは可能

（1）オフィス内の道具や設備をデジタルに置き換え

テレワークを導入するとき、多くの企業は「テレワーク用に業務を切り出そう」とします。しかし、紙や対面を含む現状の手順のままでは、切り出せる業務は限定的。そのため工程の前半をテレワークで、後半を翌日オフィスでやるなど、テレワークが非効率の原因になってしまうこともあります。

やるべきことはオフィスでの仕事の仕方をデジタル化すること。紙はデータに、対面はウェブ会議にするなど、一つ一つの仕事をデジタル化していけば、テレワークでできる仕事はどんどん増えていきます。同様に壁面の予定表はオンラインカレンダーに、ハンコは電子印鑑にと、オフィス内の道具や設備をデジタルに切り替えていくことで、どこにいても同じように仕事をすることができるようになります。テレワークはオフィスのＤＸ（デジタルトランスフォーメーション）※のチャンスなのです。

※DX（デジタルトランスフォーメーション）とは「デジタルによる変革」を意味し、ITの進化に伴って新たなサービスやビジネスモデルを展開することでコストを削減し、働き方改革などの変革につなげる施策を総称したもの

コンサルタントからのアドバイス

ペーパーレスの進め方のヒント

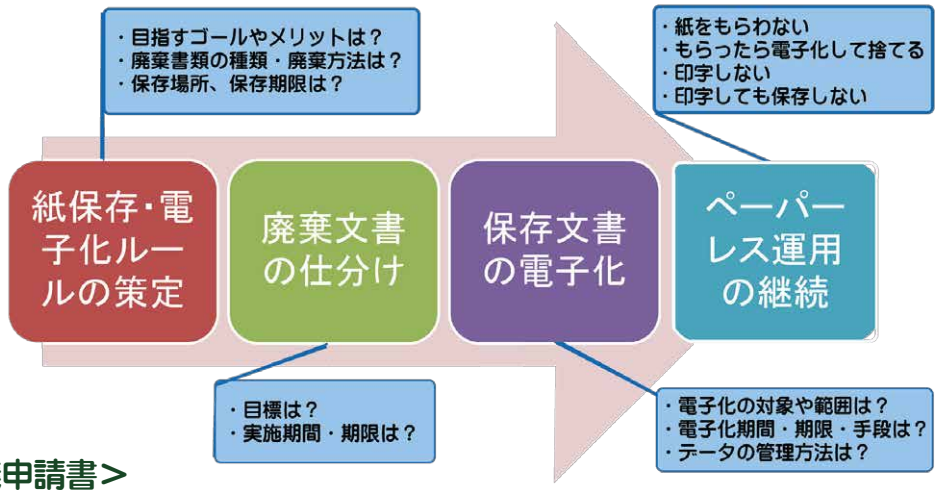
テレワーク活用のカギを握るのがペーパーレス。できるだけ今の仕事のプロセスから紙をなくし、デジタルに置き換えることを進めましょう。　紙の種類に合わせて、対策のポイントをご紹介します。

＜書類＞

①取組開始日を決めて、その日以降は紙ではなくデータを原本とします。（法律で紙保存が必要なものは除く）。

②今すでにある紙については、以下のようなプロセスで仕分け、断捨離、電子化を進めましょう。ペーパーレスで得られる具体的なメリット（たとえば、「削減できた印刷代等のコストは社員に還元」「キャビネット廃棄後はカフェコーナーを作る」等）をあらかじめ明示しておくと、従業員のモチベーションも上がります。

また、過去の書類の電子化は、一度に全部やらず、必要になったらその都度、その分だけ実施するのがコツです。



＜契約書・稟議申請書＞

クラウドで利用できる電子契約のサービスや電子ワークフロー、電子印鑑の利用が便利です。

（電子契約：「クラウドサイン」「DocuSign」等　電子印鑑：「パソコン決裁Cloud」「My電子印鑑」等）

＜請求書・経費精算＞

クラウドで利用できる経理ツールや、清算ツールの導入がお勧めです。電子帳簿保存法に対応しているサービスを利用すれば、紙保存も減らすことができます。

（請求書：「マネーフォワードクラウド請求書」「BtoBプラットフォーム請求書」等
経費精算：「楽々精算」「会計Freee」等）

各社から様々なサービスが出ているので、比較検討してみましょう。

第2章

最新セキュリティ対策

■この章では特にテレワーク時に気をつけたい、セキュリティ対策について学びます。

業務上の情報は企業にとって「情報資産」です。「情報資産」を守るためには、システムに頼るだけではなくセキュリティ対策が重要です。

まずは「ルールによるセキュリティ対策」。情報セキュリティのポリシーや情報資産の洗い出し、そして情報セキュリティ研修が必要です。

次に「技術によるセキュリティ対策」。昨今、ネットワークは全く信頼できないものとする「ゼロトラスト」の考え方が主流です。そのうえで、ネットワークと端末の管理ポイントを押さえておきましょう。

1 .ルールによるセキュリティ対策

Point

・会社の情報資産を守るには情報セキュリティポリシーが必要
・情報資産を洗い出して機密情報・業務情報・公開情報に分類

（1）テレワークをする労働者の環境、情報セキュリティ対策をチェック

企業が管理する紙文書や電子データ、各種の情報などを「情報資産」といいます。テレワーク時には「情報資産」がインターネット上を流れてやりとりされたり、社外にあるノートパソコンで利用されたりします。そのため、社内で仕事をするときよりもウイルス感染、端末の紛失・盗難、通信内容の盗聴といった「脅威」にさらされやすいといえます。

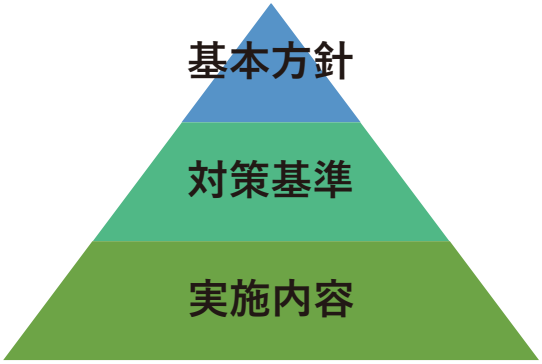
これらの脅威に対してルールによるセキュリティ対策をとるには、まずはテレワークをする労働者が、どこで、どんな機器を使って、何の情報を扱っているのかを把握することが必要です。

さらにはテレワークをする労働者が、利用する情報資産の管理責任をどのように考えているかを知る必要もあります。その上で、テレワーク時の働き方や情報の取り扱い方をルール化していきましょう。

まずは、現在のテレワークをする労働者の環境や既存の対策を正確に把握することが大切です。

（2）情報セキュリティポリシーの策定

情報セキュリティポリシーは、全体の根幹となる「**基本方針**」、実施すべきことや守るべきことを規定する「**対策基準**」、具体的に実行するための手順を示す「**実施内容**」の3階層で構成します。



テレワーク時だけに限らず、社内で働く際にも守るべき内容を定めます。

ただし、「情報セキュリティポリシー（＝ルール）」を作っただけでは、安全に働ける環境は生まれません。

「ルール」を守るべき「人」、さらにルールでカバーできないところを補う「技術」の3つの施策をバランス良く実施することが大切です。

（3）情報資産の洗い出しと格付け

情報セキュリティ対策を効率的に実施するために、まず保護すべき情報資産を洗い出し、どのような脅威や脆弱性、リスクがあるかを把握・認識します。そして、情報を重要度に応じて格付けし、それに応じた対策を行うことが重要です。

	分　類	内　容	テレワーク時のルール例
情報資産	機密情報	個人情報や顧客から預かった非公開情報、営業秘密、自社の経営に関する情報	閲覧のみ
	業務情報	機密情報には該当しない、社内打ち合せ資料、勤務管理簿、研修教材などの公開を前提としない情報	社外持ち出し可
	公開情報	ウェブサイトやパンフレットなどに掲載しているような、公開している情報	社外持ち出し可

また、さらに重要なのは、情報資産の利用者が、この格付けを識別できるようにしておくことです。電子データはフォルダによる区別、紙媒体は「機密」等と表記することで識別できるようにしておきます。

（4）情報セキュリティ研修

情報セキュリティについての各種ルールは、テレワークをする労働者にも遵守するよう求める必要があります。そのため、情報セキュリティ研修などで労働者全員に理解してもらい、浸透させることが重要です。

そして、テレワークをする労働者の認識を確実なものにするためには、一過性のものではない教育・啓発活動を日々、定期的に実施するのが効果的です。

併せて、就業規則等にテレワーク時の機密保持に関する決まりやと違反時の罰則に関する規定も定めておくのもよいでしょう。

テレワーク豆知識

情報セキュリティ10大脅威　2020脅威ランキング

「個人」向け脅威	順位	「組織」向け脅威
スマホ決済の不正利用	1位	標的型攻撃による機密情報の窃取
フィッシングによる個人情報の詐取	2位	内部不正による情報漏えい
クレジットカード情報の不正利用	3位	ビジネスメール詐欺による金銭被害
インターネットバンキングの不正利用	4位	サプライチェーンの弱点を悪用した攻撃
メールやSMS等を使った脅迫・詐欺の手口による金銭要求	5位	ランサムウェアによる被害
不正アプリによるスマートフォン利用者への被害	6位	予期せぬIT基盤の障害に伴う業務停止
ネット上の誹謗・中傷・デマ	7位	不注意による情報漏えい（規則は遵守）
インターネット上のサービスへの不正ログイン	8位	インターネット上のサービスからの個人情報の窃取
偽警告によるインターネット詐欺	9位	IoT機器の不正利用
インターネット上のサービスからの個人情報の窃取	10位	サービス妨害攻撃によるサービスの停止

テレワークQ&A

情報漏洩は他人事ではない！？

「うちは、サイバー攻撃を仕掛けられるような情報はもっていませんから、大丈夫ですよ」

とおっしゃる社長さんがいらっしゃいますが、それは大きな勘違いです。

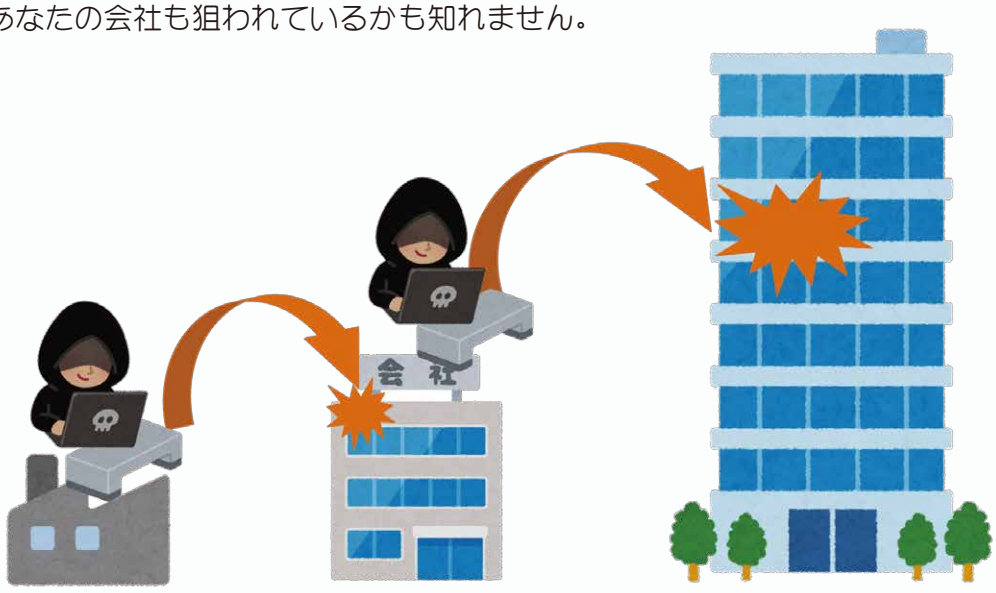
今や、セキュリティ対策が手薄な企業こそ狙われているのです。

前のページの「テレワーク豆知識」でご紹介した「情報セキュリティ10大脅威 2020脅威ランキング」の「組織」向け脅威の4位に「サプライチェーンの弱点を悪用した攻撃」とあるのが、まさにそれです。実際に、2019 年に日本スポーツ協会の新システム開発の再委託先が不正なアクセスを受け、動作検証用に構築したサーバー内のデータベースから個人情報が削除された。という被害がありました。

攻撃者は最も手薄な企業を狙い、そこを踏み台にして次々とシステムに侵入し、目指す大企業に飛び移っていくのです。踏み台にされた企業は被害者であるとともに、加害者にもなってしまいます。

例えば自社の従業員のパソコンがウィルスに感染しており、そこからお客様にウィルスを含むメールや納品物が送られ、それによってお客様が被害を受けるようなことになれば、損害賠償責任は免れないでしょう。

企業規模はセキュリティの必要性とは関係ありません。どんな小さな企業でも自社の環境、あるいは自社の委託先の環境も含めてしっかり確認し、十分な対策をとっておきましょう。
あなたの会社も狙われているかも知れません。



2.技術によるセキュリティ対策

Point

・「ゼロトラスト」の考え方による多層防御が重要
・「エンドポイント」の管理は「EPP」と「EDR」を組み合わせて実施

1）コロナ禍で起きた課題と求められる対策

2020年4月に新型コロナウィルス感染防止のための緊急事態宣言が発令されたことで、多くの企業は急遽テレワークに取り組むことになり、さまざまな課題が浮き彫りになりました。

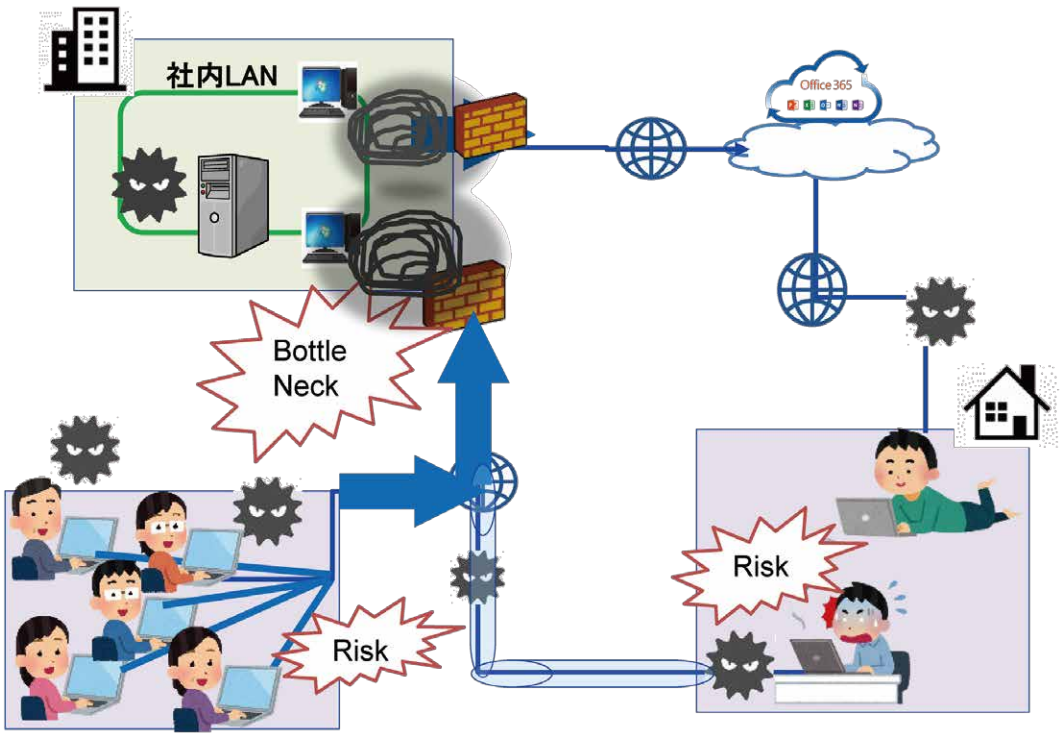
1. 多くの労働者がテレワークに移行したため、会社の通信インフラやVPNサービスの契約数が十分でなく、始業時に会社にアクセスできない人が続出

2. 私物端末や会社が許可していない通信方法で業務をすることで、ウィルス感染などのリスクが増大

3. 労働者が社外でウィルスに感染。そのパソコンで社内にアクセスをしたことで社内にも感染が拡大してしまった。

このような現象を受け、従来のように会社を境界で守り、その中に入ってきたアクセスは安全とみなす、という考え方ではなく、すべての端末・アクセスは無条件に信頼せず検査・監視するという「ゼロトラスト」という考え方に注目が集まっています。

ゼロトラストでは、ネットワークの環境とエンドポイントと呼ばれるユーザーの環境を重点的に管理します。

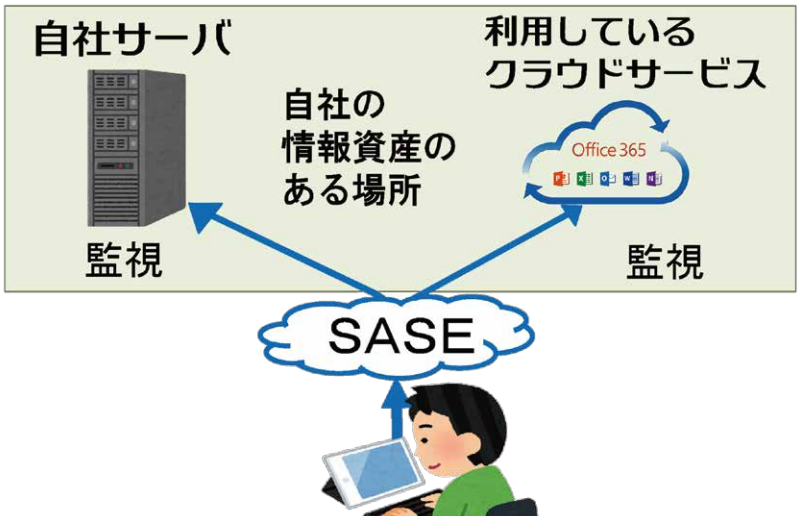


(2) ネットワークの管理

「ゼロトラスト」では、社内を安全な場所とは考えず、通信アクセスをすべて可視化、検証したり、すべての通信のログを残し、監視したりします。ユーザーには必要最低限のアクセス許可しか与えません。

「ゼロトラスト」を実現する基盤としては、SASE(Secure Access Service Edge)と呼ばれる、通信と監視をワンストップで提供するクラウドサービスがあります。

すべてのユーザーはまずそのクラウドにアクセスして、そこから必要なデータにアクセスします。もちろんすべてのアクセスは監視・管理されます。今後は拠点ごとにVPN通信を構築するような仕組みに代わり、このような製品の導入が進むと考えられます。



(3) エンドポイントの管理

テレワークをする労働者が自宅で使用する端末などを指す「エンドポイント」の管理が、セキュリティ対策には重要です。「エンドポイント」のセキュリティは、大きく「エンドポイント保護プラットフォーム＝EPP」と「エンドポイントの検知・対応＝EDR」の2つに分けられます。

EPP(Endpoint Protection Platform)	EDR(Endpoint Detection and Response)
パソコンなどがマルウェア(＝悪意のあるソフトウェア)に感染しないように防止する製品	**EPPではマルウェアを検知できず感染してしまった場合に脅威を検知し、報告する製品**

EPPで阻止できなかった攻撃を EDRで対応するという、これらを組み合わせた多層防御が「エンドポイント」の管理のポイントです。

第3章

効果的なコミュニケーションメソッド

■この章ではテレワーク時に有効な、コミュニケーション方法について学びます。

テレワークでも普段と同じコミュニケーションをするには、適切なツールを導入し、まずはそれを全員が使えるようにしましょう。そしてさらにコミュニケーションの質を高めるためには、状況に合わせてツールを使い分けたり、利用ルールを定めて、無駄なく活用していくことも必要です。

また、テレワークを快適に実施するためには、基本的なマナーを守り、テレワークでのハラスメント、いわゆる「テレハラ」にならないよう、十分気をつけましょう。

1.チームの一体感を高めるコミュニケーションツール

Point

・スピーディーにやり取りできるチャットは、多くの企業で導入されている
・状況に合わせてチャットとメールを使い分けて活用していくことが重要

（1）社内コミュニケーションはメールからチャットへ

最近では多くの企業で導入されているチャットの最大のメリットは、会話をしているようにスピーディーにやり取りができることです。スタンプを活用すれば、さらに素早く相手に気持ちが伝わります。チャットのタイムライン（ツールの画面上）には、過去に交わしたメッセージが残るため、会話の流れを視覚的に確認しやすいという利点もあります。重要な発言には「ピンどめ」する機能などを利用すれば、見返すことも簡単です。

チャットで送ったメッセージは修正や削除ができるため、誤送信をしても、素早く対応すれば情報漏えいが回避できることもあります。

また、プロジェクトごとや部署ごとにグループチャットをつくり、そこでやり取りをすることで、情報の共有漏れがなくなります。

メールのメリットは、長文で用件を伝えられること。多くのメールソフトでは、件名、アドレス、キーワードなどから過去メールが検索できるため、受送信したメールを簡単に検出できます。確実に記録に残しておきたい情報は電話やチャットではなく、メールでのやり取りをおすすめします。ただし、自分でフォルダを分けないとすべてのメールが1か所に入ってきてしまうため、大事な要件が埋もれてしまうリスクがあります。

チャットの特徴

メリット

*定型文などなく短い文章ですむ
*スピーディに意思の確認、疎通ができる
*やりとりの流れが視覚的に確認しやすい
*複数人でのコミュニケーションが容易
*伝え忘れ、伝え漏れを防ぐことができる
*外部のサービスやツールと連携できる
*送ったメッセージを削除、編集できる
*スタンプが使える

デメリット

*メッセージがタイムラインに埋もれてしまう
*相手が限られる
（同じツールがないと利用できない）

メールの特徴

メリット

*基本的に読むタイミングを限定しない
*送る側・受け取る側の時間を拘束しない
*履歴の検索がしやすい
*同時にたくさんの人に送ることができる
*デジタルデータのため加工や二次利用がしやすい
*コストがかからない

デメリット

*挨拶文の挿入や定型文が存在する
*送信したメールは取り消せない・情報が残る
*読まれたかどうかの確認がしにくい
*時間の共有ができない
*文字だけでのやり取りなので誤解が生じやすい
*ウィルス感染のリスクがある