Ｐマーク(個人情報保護) ガイドブック

（スタッフ）　　JISQ15001:2023 準拠

2025年6月

株式会社スタッフアイ

《 目　次 》

■別冊「STAFF GUIDE BOOK」(スタッフガイドブック)も併せてご覧ください

「8. 個人情報保護(P.23～P26)」　「9. 守秘義務(P27～P28)」

1. プライバシーマーク・個人情報保護マネジメントシステム

■「プライバシーマーク」とは

・個人情報を適切に取り扱っているつもりでも、それを自社で証明することはできない。第三者により認定してもらう制度が「プライバシーマーク制度」である。
・プライバシーマーク制度は、審査機関により審査され、一定の基準を満たすことで認定された事業者に対し、プライバシーマークが付与される。(2年ごとに審査を受ける)

■「個人情報保護マネジメントシステム」とは

・「個人情報保護マネジメントシステム」は個人情報保護に特化したマネジメントシステムであり、JISQ15001 に準拠した PDCA を回していく仕組み。
・個人情報保護マネジメントシステムを構築、運用していることがプライバシーマーク取得のための条件である。
・略称として、PMS(Personal information protection Management System)とも言う。

2. PMS教育の重要性

・PMS を維持し、更新していく上で、「教育」には、とても重要な意味がある。
・会社の個人情報保護レベルは、最も認識が低い従業者レベルとイコール。
・従業者一人ひとりの意識の向上と日常の取り組みが会社を支えている。

◆従業者(役員、社員、契約社員、派遣社員等を含む)を対象に年１回以上実施する。
◆受講者には、本冊の内容を理解できたかどうかを確認するために理解度確認テストを実施する。

3. PMS 教育のポイント

①個人情報保護方針の周知
②PMSに適合することの重要性、遵守することによる利点
③PMSに適合するための役割、及び責任
④PMSに違反した際に予想される社会的な影響、企業経営への打撃、違反した当事者の処分・賠償責任など

4. スタッフアイの「個人情報保護方針」

個人情報保護方針

株式会社スタッフアイは、人材派遣、人材紹介、受託業務、並びにその他の事業を行うにあたり、個人情報の重要性を認識し、保護することを社会的責務と考えております。当社で業務に従事する全ての者が、個人情報を保護することを事業運営上の最重要事項の一つと位置付け、個人情報に関する法規制、及び業界の指導を遵守し事業活動を行うことにより、社会の信頼にこたえてまいります。

記

1. 個人情報は、当社事業活動に必要な範囲に限定し収集、利用、提供、及び預託を行います。個人情報収集にあたり、情報提供者の同意を得るものと致します。
   また、受託業務においては業務の範囲内の利用とします。また目的外の利用を行わないものとし、そのための措置を講じます。

2. 当社が事業活動に必要な為に保有する個人情報(当社が取得し、又は取得しようとしている個人情報を含む)の漏洩、滅失、及びき損などを防止するため、合理的な安全対策是正及び予防措置を講じます。

3.個人情報保護に関する法令、国の定める指針、その他の規範、及び業界の指導を遵守致します。

4.個人情報、個人情報保護マネジメントシステムに関する本人からの苦情、及び相談に対応致します。

5.個人情報保護マネジメントシステムは、その内容を継続的に見直し、改善を行います。

6.この方針は、役員をはじめとする全従業者に配布し周知するとともに、社外の第三者に対しても公開致します。

以上

最終改訂　2024年 4月 1日
制定　2003年 5月13日
株式会社スタッフアイ

■個人情報の取扱に関するお問合せ先　管理部長　tel.0120-454-353　e-mail:info@staffi.co.jp

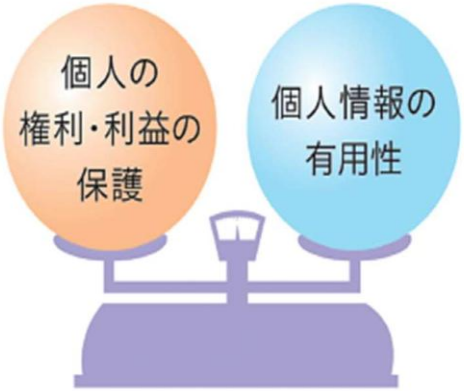
5. 個人情報保護法

・デジタル技術が飛躍的に進歩し、経済・社会活動のグローバル化に伴い、個人情報を含むデータの国境を超えた流通が増えている。
・個人情報に対する人々の意識が高まっており、利用者の安心、安全、信頼を確保されることが求められている。
・個人情報保護法は、社会の変化に対応できるように、３年を目途に見直しが必要と定められており、直近、2023 年４月１日から改正法が全面施行。

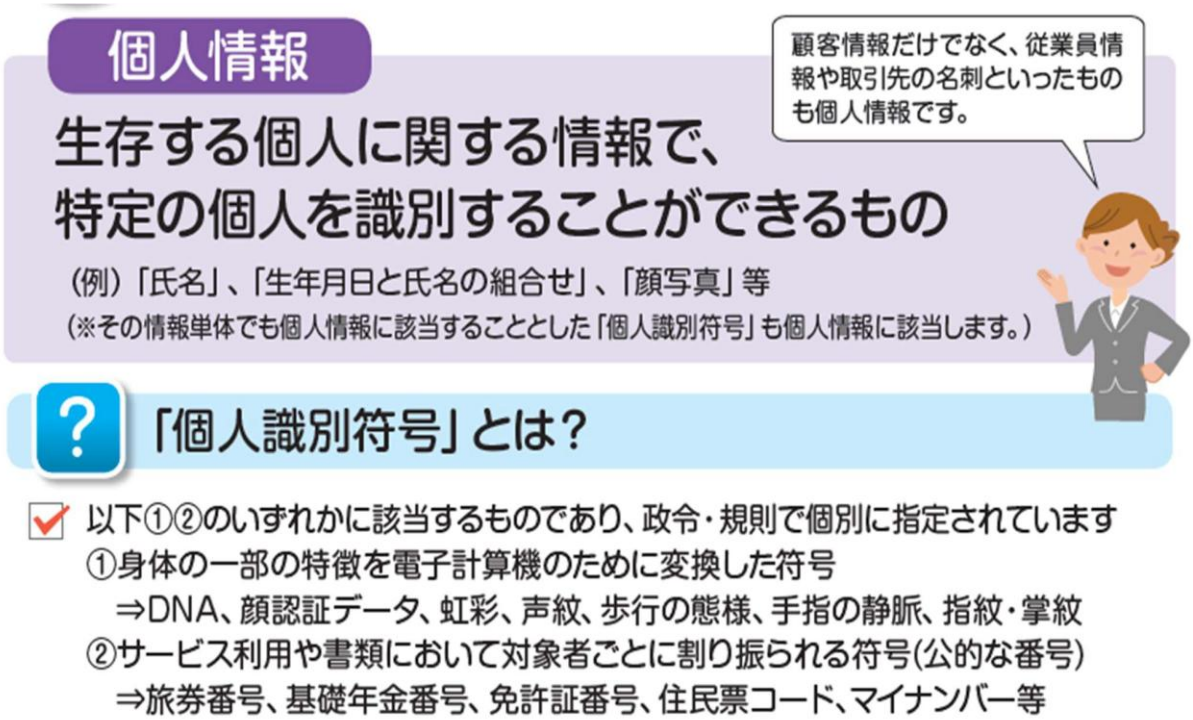
■「個人情報保護法」とは

2017年5月30日から、すべての事業者に「個人情報保護法」が適用される！

- ☑ 個人の権利・利益の保護と個人情報の有用性(社会生活やビジネス等への活用)とのバランスを図るための法律
- ☑ 民間事業者の個人情報の取扱いについて規定
- ☑ 従来は、取り扱う個人情報の数が5,000人分以下の事業者には適用されていませんでしたが、平成29年5月30日からは、すべての事業者に適用されています



■「個人情報」とは



☑ 以下①②のいずれかに該当するものであり、政令・規則で個別に指定されています
①身体の一部の特徴を電子計算機のために変換した符号
⇒DNA、顔認証データ、虹彩、声紋、歩行の態様、手指の静脈、指紋・掌紋
②サービス利用や書類において対象者ごとに割り振られる符号(公的な番号)
⇒旅券番号、基礎年金番号、免許証番号、住民票コード、マイナンバー等

■「守秘義務」とは

職場には、経営に関すること、顧客に関すること、または一緒に働く人たちの個人情報など重要な情報がたくさんあります。従業者の皆様からこれらの情報が外部に漏れることは絶対にあってはならないことです。これらを守秘義務と言い、契約終了後も継続します。

個人情報、会社情報、機密情報や派遣先の各情報を含めて、雇用契約・業務契約等の契約期間中はもとより契約終了後も一切第三者に開示又は漏えいしてはならない。

◇守るべき PMS ルール

(※)②～④は個人情報をデータベース化(特定の個人を検索できるようにまとめたもの)した場合にかかるルールです。
なお、これらの個人情報データベース等を構成する個人情報を、「個人データ」といいます。

6. PMS に適合することの重要性、遵守することによる利点

(1) プライバシーマークとは、**個人情報の取扱いを適切に行っている事業者に与えられる「信頼と安心」のマーク**です。
プライバシーマークを取得し「目に見える形での安心の提供」が出来ることは、「お取引先様や登録者・派遣スタッフへの信頼獲得」の最も効果的な手段と考えます。
自分の個人情報を自分で守る為には、安心して個人情報を預けられる会社を選択することが重要で、その選択される会社であることの証明となります。

(2) プライバシーマーク制度は、「**財団法人日本情報処理開発協会(JIPDEC)**」が運営している、**JISQ15001:2023(個人情報保護に関するJIS)に適合した PMS** を整備し、個人情報の取扱いを適切に行っている事業者を評価・認定し、その証として「プライバシーマークの使用を許諾」(マーク使用許諾証を授与)する制度で、属人的ではなく組織的な個人情報保護対策ができ、実施したことを記録として残すことができます。

(3) 個人情報保護への意識を高めるため、また業務の標準化を進める上で、有効なツールとなります。

7. PMS に違反した場合の影響

個人情報保護法の成立以来、個人情報保護への社会的関心は高まっており、新聞、インターネット上では、ほぼ毎日のように個人情報に関わる事件、事故のニュースを目にする様に以下の影響がある。

1)当社で重大な個人情報事故が起きると、会社の情報管理能力を疑われ、社会的なイメージダウンや、顧客からの信用低下を引き起こし、今後の経営に致命的なダメージを与えてしまう。
2)事故の内容や規模によっては、顧客に対して多額の損害賠償支払い、営業自粛といった金銭的な影響も発生する可能性がある。
3)PMS に違反した場合、就業規則に従い、懲戒処分の対象となる場合がある。

8. 安全管理のための基本ルール

※派遣先のルールを確認

(1)盗難の防止

・離席時及び退室時はクリアデスクを徹底する。
・離席一定時間後、PCはパスワード付きスクリーンセーバー又はログオフ設定とする。
・名刺は所定の名刺Box又は名刺フォルダに入れて保管する。
・個人情報記録していたPCを廃棄する場合、派遣先の指示に従いデータ消去を行う。
・個人情報保存のノートPCは退出時、施錠できるキャビネに保管する等の対策する。
・個人情報を記録媒体(USB メモリ、DVD、ポータブル HDD 等)に保存する場合は派遣先の指示に従う(暗号化又はパスワードを設定する等)。

(2)PC、情報システム、情報サービスのアカウント、パスワード

・アカウントには必ずパスワードを設定する。
・パスワードは複雑なものにする。
・パスワードは以前に使用した同一あるいは類似するものは使用しない。
・パスワードは付箋等で場面の横等に貼り付けない。
・パスワードは本人が設定し、他人には教えない。
・漏えいした、又は漏えいの恐れがある場合、パスワードは速やかに変更する。

(3)PCの不正ソウトウェア対策

・PCにウィルス対策ソフトウェアを導入する。(ウィルス対策ソフトウェアとファイアーウォールの役割は異なる)
・ウィルスパターンファイル、プログラム更新は、常時最新版を運用する派遣先に確認する。
・セキュリティ対策用修正ソフトウェアは常時最新版を適用する様派遣先に確認する。
・業務遂行上必要なソフトウェア以外の利用は禁止しない。
・業務遂行上、新たなソフトウェア導入が必要になった場合、派遣先の指示に従う。
・ファイル交換ソフトウェアの利用は禁止する。

(4)個人情報の移送、通信時の対策

・重要な個人情報を発送する時、書留郵便、追跡付き宅配サービス等を使用する(派遣先のルールに従う)。

・個人情報を受託業務で預かる時、委託業務で預ける時、第三者から受け取る時、第三者に提供する時には授受記録を残す等派遣先の指示に従う。

・個人情報を含むデータを取り扱う際には適切なセキュリティ対策を行う。

(5)FAX利用管理

・FAX送受信後、速やかに回収し、放置しない。

(6)メール利用管理

・業務目的以外のメール使用は禁止する。

・送信前に送信先アドレスに間違いがないことを確認する。

・複数のメールアドレスに同じメールを送信する場合、送信先アドレスが受信者間で閲覧できないようにBCC送信する。(派遣先のルールを確認)

(7)Webサイト利用管理

・業務目的以外でのWebサイトへのアクセスは禁止する。

・運営元の明らかでない信頼性の低い Web サイトへのアクセスは禁止する。

9. 派遣先での安全管理基本ルール

※派遣先のルールを確認

(1) 入館証、セキュリティーカードの管理

派遣先によっては就業場所に入るために入館証やセキュリティーカードを発行している場合は、紛失等などが無い様に管理には十分注意をして下さい。紛失した事による影響は、派遣先は勿論のことスタッフアイや社会に対する影響は図り知れません

(2) 指定機器、指定ソフトウェア以外の使用禁止

派遣先のお仕事は、派遣先から指定された機器や環境(PC、ネットワーク等)を使用し、指定された手順に従って業務を遂行して下さい。便利なソフトウェアやツールがたくさんありますが、それらを皆さん個人の判断で勝手にインストールしたり、使用したりしてはいけません

(3) 情報システムの私的使用の禁止

派遣先の情報システムやインターネット、E-mailを私的な利用目的で使用することは、厳禁です

(4) 送信先の確認

業務を遂行する上でE-mailやFAXを利用し、情報を派遣先外へ送信する場合、送信宛先に間違いが無いことを確認すると共に、相手先へ受信確認を行うなどの注意を常に心がけましょう。特にE-mailで複数の宛先に送信する際は、必ずBCCを利用(派遣先指示確認)するなど細心の注意が必要です

(5) 個人所有機器の持ち込み禁止

個人所有のPCはもちろん、電子記録媒体(CD-R、DVD-R、USBメモリ、SDカード等)を派遣先に持ち込んではいけません。携帯電話の使用や持込制限がある派遣先もありますので、注意して下さい

（6）離席時の注意
離席するときは、使用している PC の画面や机上の書類を片付け、他の人の目についたり、使用されたりしないように注意して下さい(クリアデスク、クリアスクリーン)

（7）情報の複写、持ち出しの禁止
派遣先の情報をみだりにコピーしたり、許可無く持ち出したり、電子メールで転送したりすることは厳禁です

（8）情報の持参時の注意
派遣先の指示により業務を遂行する上で、情報を派遣先社外へ持ち出したり、送付したりする場合は、情報の漏洩、紛失、破壊などの事故が起こらない様、細心の注意を払って下さい。特に、電車を使って移動する場合は、情報を入れたカバンや手さげの置き忘れに注意して下さい

（9）業務の持ち帰りの禁止(除く、在宅勤務)
いくら仕事熱心でも、派遣先の仕事を自宅に持ち帰ったり、電子メールで転送したりしてはいけません。最近の情報漏洩事故の多くが、会社の仕事を自宅に持ち帰り、個人の PC を使用し処理をすることが原因となっています
もしも派遣先から、仕事を自宅に持ち帰って処理するよう指示された時は、派遣元(スタッフアイ)から禁止されている旨を説明して下さい。そのことにより支障が生じた場合は、直ちにスタッフアイの営業担当者にご相談下さい。営業担当者が対応致します

（10）公共の場での発言
飲食店や居酒屋、トイレなど不特定多数が出入りする場所での機密情報の発言は避けて下さい。誰かが耳を傾けているかもしれません
また、給与など契約内容に関することについても口外しないで下さい。働く上での最低限のマナーでもあります

（11）情報の守秘義務
家族や友人のように相手をよく知っている場合でも、相手が情報を漏洩する可能性はあります。また相手が意識せずに漏洩してしまう例もありますので、機密情報、個人情報は他言しないようにして下さい

（12）用済み情報の処理
用済みとなった情報の処理は、派遣先の指示に従って処理をして下さい

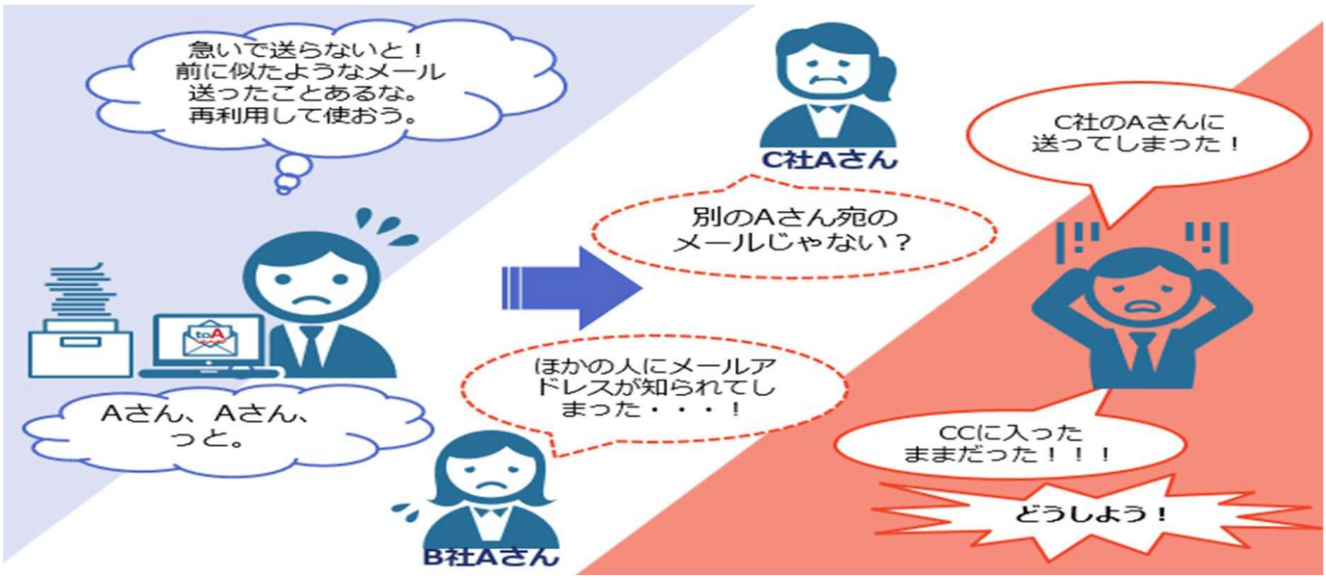
（13）事故発生時の対応
情報の漏洩、紛失、破壊、改ざん等の事故発生、またはその恐れを感じたときは、直ちに派遣先に報告し指示を受けて下さい

（14）契約終了時の情報の処理
派遣契約が終了し、退職する場合の派遣先 PC データや、預かった派遣先の情報の処置は、必ず派遣先の指示と手順に従って下さい。皆さん個人の判断で処理する事がないようにして下さい。

■万一、個人情報を紛失・漏洩した場合の対応

1)会社に報告(自己判断厳禁)
・勝手に個人判断せず、派遣先上司及びスタッフアイへ報告。
2)警察、交通機関に連絡(社外での発生時)
3)何を紛失・漏洩したかを洗い出す。
・日頃から、どのような個人情報を取り扱っているか意識する。
4)セキュリティ事故の報告書を作成
・PMS の手順に従い、原因究明、対策を検討し、記録に残す。

10. メールの誤送信に注意！「とある日常・・・から一転」



メールの誤送信に注意！「ミスの防止策(1)」

■ メール本文への対応
- □過去に送信したメールを再利用しない。
- □メール本文に個人情報を極力記載しない。
- □送信する際は、毎回ひな型からコピー＆ペーストする。
- □ひな型に上書き保存していないことを確認する。
- □取引先別にPC（担当者）を分ける。

■ 添付ファイルへの対応
- □ファイル添付ができる環境（担当者、PC）を限定する。
- □添付するファイルの保存場所を固定する。
- □一括送信時のファイル添付を禁止する。

万が一、誤送信が発生した場合に備えて
- 送りたいファイルをパスワードをつけて暗号化する。
- パスワードは簡易なものにしない。
- パスワードを相手に伝えるためには別の通信経路で送る。

送りたいファイルに上記の対策をした上で、ファイル転送サービスなどを利用する手段もあります。

メールの誤送信に注意！「ミスの防止策(2)」

■ アドレス帳からの選択ミス防止
- □企業名、氏名等をわかりやすいように登録する。
- □取引先部署ごとなど、分類を細かくする。

■ アドレスの入力ミス防止
- □送受信の確認が済んでいるアドレス帳を使用する。
- □複数の担当者で確認する。

■ 送信先アドレス欄の選択ミス防止
- □送信先はBCCにしか入力できないようにする。

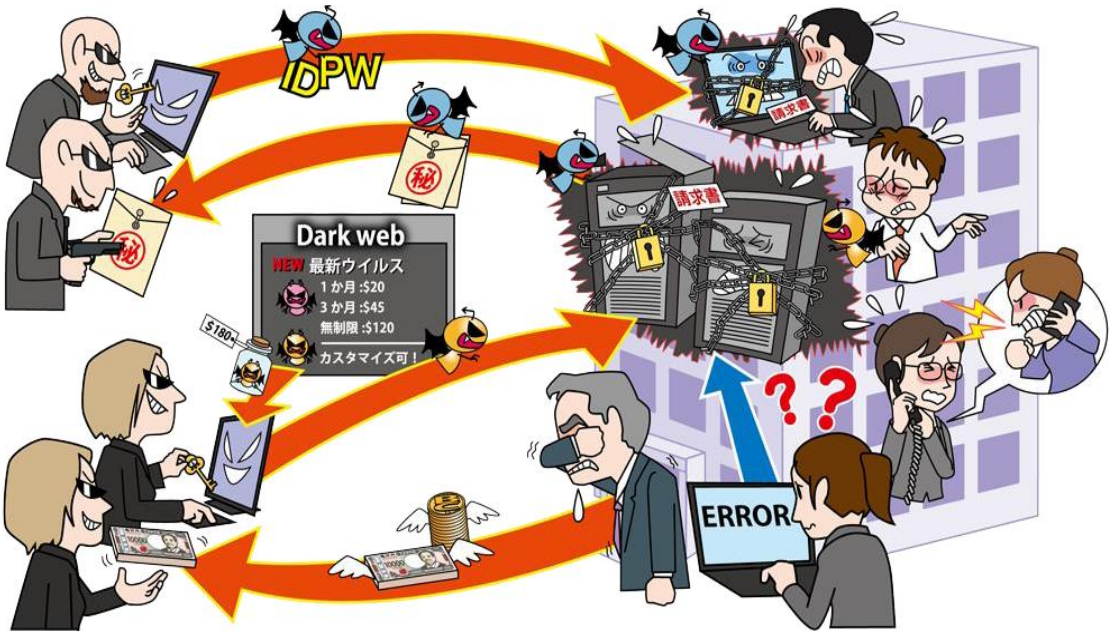
■ その他
- □メーリングリストを活用する。
- □メール作成者と送信者を分けて、送信先確認をする。

メール送信前の再確認、ダブルチェックを徹底する

11.「情報セキュリティ 10 大脅威　2025」

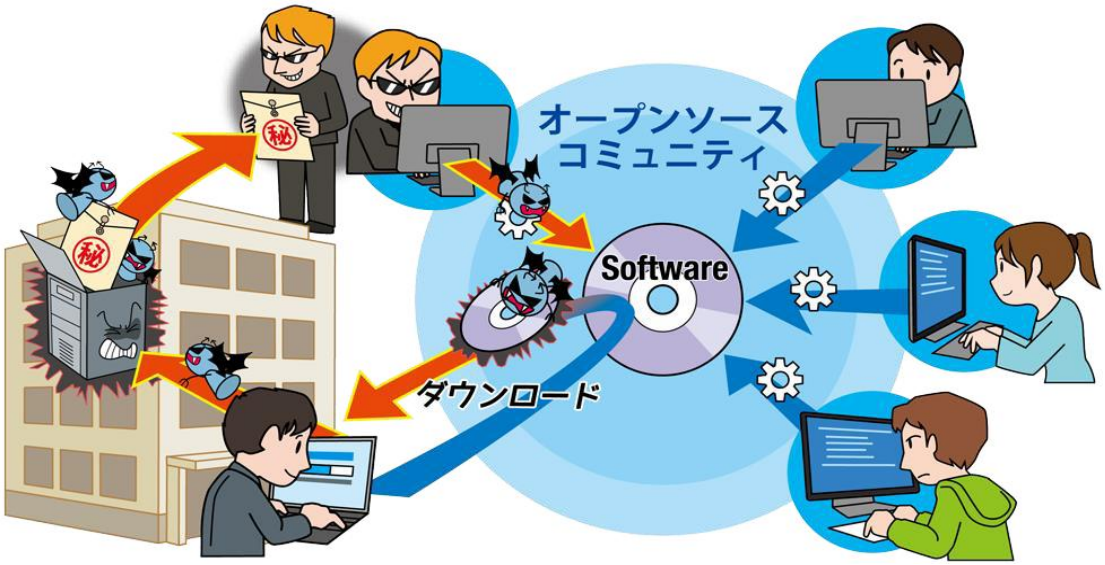
※独立行政法人情報処理推進機構(IPA)が提供の情報。（第１位～第３位の脅威を抜粋）

１位 ランサム攻撃による被害



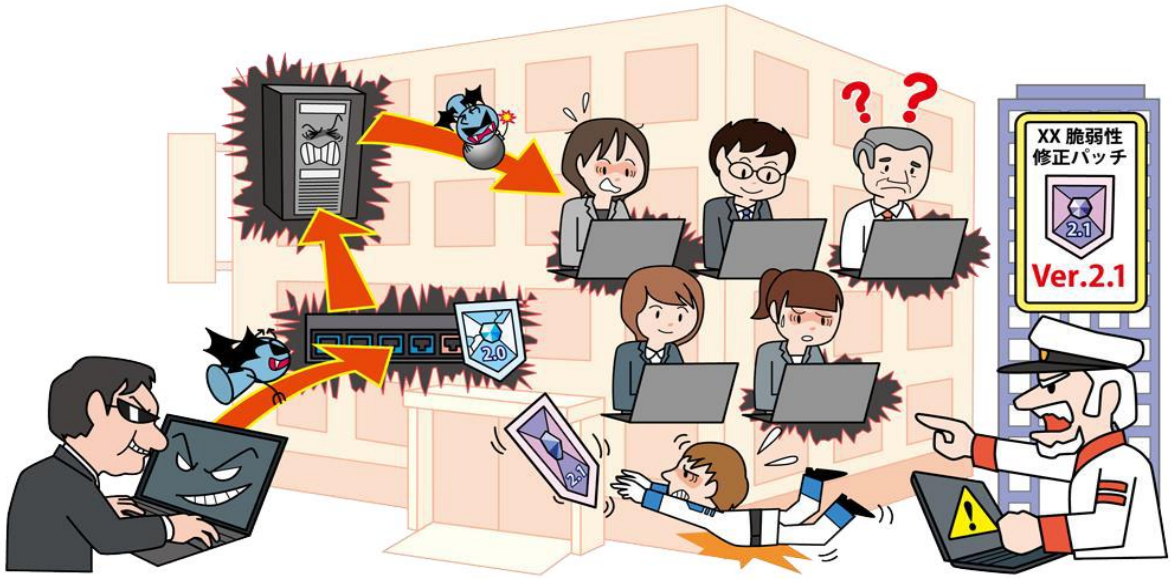
ランサムウェアとは、PC やサーバーに感染後、端末のロックやデータの窃取、暗号化を行い、これらを取引材料とした様々な脅迫により金銭を要求するマルウェアの一種である。ランサムウェアを用いた攻撃をランサム攻撃と呼び、攻撃者は複数の脅迫を組み合わせて、被害組織が金銭の支払いを検討せざるを得ない状況を作り出そうとする。また、近年では RaaS(Ransomware as a Service)という、サービスとして開発・提供されたランサムウェアを利用して攻撃を実行する形態も確認されるほか、ランサムウェアによる暗号化を行わず、窃取した機密情報を公開すると脅迫して金銭を要求する「ノーウェアランサム」による攻撃も確認されている

２位 サプライチェーンや委託先を狙った攻撃



商品の企画、開発から、調達、製造、在庫管理、物流、販売までの一連のプロセス、およびこの商流に関わる組織群をサプライチェーンと呼ぶ。このような「ビジネス上の繋がり」を悪用した攻撃は、自組織の対策のみでは防ぐことが難しいため、取引先や委託先も含めたセキュリティ対策が必要な脅威と言える。また、ソフトウェア開発のライフサイクルに関与するモノ(ライブラリ、各種ツール等)や人の繋がりをソフトウェアサプライチェーンと呼ぶ。このような「ソフトウェアの繋がり」を悪用した攻撃もまた脅威であり、対策が求められる。

3位 システムの脆弱性を突いた攻撃



製品の開発ベンダー等による脆弱性対策情報の公開は、脆弱性の存在や対策の必要性を製品利用者に対して広く呼び掛けることができる。他方、攻撃者はその情報を悪用し、脆弱性対策が講じられていないシステムを狙って攻撃を行うことがある。なお、脆弱性対策情報を公開する前に行われる脆弱性を悪用した攻撃をゼロデイ攻撃と呼ぶ。脆弱性対策ができていない場合、マルウェア感染等に留まらず、事業やサービスの停止等に端を発し、甚大な被害に至ることもある。昨今、脆弱性が発見されてから、それを悪用した攻撃が発生するまでの時間が短くなっているため、脆弱性対策情報が公開された場合、早急な対策の実施が求められる。

END