国民のための
サイバーセキュリティサイト

総務省

事前対策

（セキュリティ事故を未然に防ぐためには）

システムを“管理”する人向けの対策

情報管理担当者は、情報セキュリティポリシーで定めた事項が組織全体で実際に実行されるように、情報システムの管理・運用や、社員・職員に対する教育・監督を適切に行う必要があります。
また、情報通信技術の進歩は早く、企業・組織の情報資産を脅かす新しい脅威が次々に登場しています。よって、情報管理担当者には、これらの脅威について情報を収集し、必要に応じて組織幹部や外部の専門家とも連携しながら、継続的に組織全体の情報セキュリティ体制を見直していく役割も期待されています。

ここでは、企業・組織における情報管理担当者が実践すべき情報セキュリティ対策について説明します。
既に組織内で情報セキュリティポリシーが策定されている場合には、その内容を元にして情報セキュリティ対策を進めるようにしてください。

目次

情報セキュリティ関連文書の整備

既に情報セキュリティポリシーを導入している企業や組織、これから導入を検討している企業や組織の情報管理担当者として、以下の点に十分留意しなければなりません。

- 高度にネットワーク化した情報システムは、情報資産への脅威を招くなど負の側面があるが、適切な情報セキュリティ管理を行うことにより、大きな利便性を与えるものでもあることを認識する。
- 企業や組織として意思統一され、明文化した情報セキュリティポリシーを策定する。
- 企業や組織として情報資産の重要度を分類、評価して、守るべき情報資産のレベルに応じた情報セキュリティ対策を情報セキュリティポリシーに反映する。
- 情報セキュリティ対策が「いかに破られないか」という予防の視点のみならず、「破られたときどうするか」という対応の視点も情報セキュリティポリシーに盛り込む。
- 情報セキュリティポリシーは、「計画」、「導入・運用」、「評価」、「見直し」をひとつの実施サイクルとし、このサイクルを止めることなく実施していく。
- 「評価」、「見直し」の手法として、情報セキュリティ全般に関する組織監査や、ネットワークやサーバの情報セキュリティ監査を取り入れる。
- 情報セキュリティポリシーの導入に際しては、社員や職員の教育、啓発の実施方法を十分に考慮する。

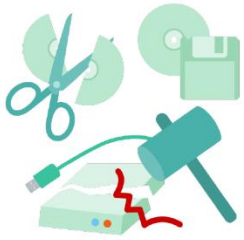
以上のような留意点に基づき、情報セキュリティポリシーを積極的に社員や職員に普及させ支援する、情報セキュリティポリシーが遵守され、有効に機能しているか、業務の妨げなどになっていないかなどを日常的にモニタリングする、情報セキュリティ対策の評価を行い、経営幹部へ報告を行うなど、情報セキュリティポリシーの導入だけでなく継続的に運用を行うことが必要です。

安全なデータ・端末の廃棄

廃棄した物品からの情報漏洩を防ぐには、パソコンや記憶媒体は、必ず情報管理担当者が取りまとめて適切な処理をした後で廃棄するなど、社内で統一の手順とルールを確立し、徹底することが重要です。

なお、パソコンなどをリースしていて期間終了に伴い返却する場合は、リース会社においても適切に処理されるよう、契約内容に含めることも重要です。

不要になったコンピュータのハードディスク・SSD や記憶媒体の処理方法には、次のようなものがあります。



■ データ消去用のソフトウェアを利用する

データ消去用のソフトウェアを利用すると、ハードディスクやメディアのファイルを無意味なデータですべて上書きするなどして、二度と復元できないように完全に消去することができます。なお、SSD についてはその特性からハードディスク用のデータ消去ソフトでは完全に消去できない場合があるので、専用のソフトを使用するか物理的な破壊などを検討しましょう。

■ 専門業者のデータ消去サービスを利用する

専門業者にデータ消去を依頼する場合には、消去する前の重要なデータをその業者に渡すことになります。依頼先の会社の実績や信頼度、さらにその会社におけるプライバシーポリシーのあり方にも考慮して業者を選定しましょう。

不適切な業者に委託したために、データ消去・廃棄されるはずのハードディスクが転売され、情報漏洩につながった事例もあるため、特に留意が必要です。

■ ハードディスクや記憶媒体を物理的に破壊する

ハードディスクについては、外側のケースを破壊しても、中にあるディスク自体が破損していない場合があります。このまま廃棄すると、ディスクを取り出してデータを復元できることもあ

るので、データが記録されているディスク面が確実に破壊されたことを確認しましょう。
CD、DVD などの記憶媒体については、メディアを破壊するために利用できるメディア専用のシュレッダで粉砕しましょう。

■ 「暗号化消去」を行う

ハードディスク・SSD の記録を暗号化していた場合は、復号に必要な鍵を確実に廃棄することにより、記録内容を読み出せなくする方法があります。これにより、上書き消去漏れ、物理的破壊漏れによるデータの復元リスクもなくせます。

例えば、Windows OS において利用可能なストレージ暗号化方式である BitLocker の場合、保管している回復キーを確実に廃棄することで実現します。留意すべきは、第三者が回復キーを入手する可能性を排除するために、回復キーを保存したデバイスを廃棄する場合はパソコンと一緒に廃棄してはいけないということです。

暗号化消去は「政府機関等のサイバーセキュリティ対策のための統一基準群（令和 3 年度版）」で追加されました。

ソフトウェアの最新化・脆弱性管理

ソフトウェアを導入する際には、その時点での最新版を使用することが適切な対応ですが、時間の経過とともに新たな脆弱性（ぜいじゃくせい）が発見されるため、情報管理担当者はソフトウェアを常に最新にする対応を行う必要があります。

ソフトウェアの開発元やシステム機器メーカーから、ソフトウェアに対する更新プログラムが配布されることがあります。更新の内容には、ソフトウェアへの機能の追加・修正や、脆弱性の修正などがありますが、特に脆弱性の修正に関するものについては日々注視しておく必要があります。

脆弱性の修正に関する更新が発表されたときは、まず自分が管理するシステムについての影響や緊急性を検討します。特に、外部に広く公開している Web サーバなどに深刻な脆弱性が発表されたときは、迅速な判断と対応が求められます。不正アクセスなどの被害を受けないよう、事前に行うべきことや作業の手順を確認し、可能な限り迅速に更新プログラムを適用しましょう。

また、脆弱性を有することのみが先に発表され、メーカーなどが修正プログラムを作成するまでに時間を要することもあります。そのような場合は、修正プログラムが発表されるまでの間は、一時的回避策を適用してシステムを保護し、修正プログラムが発表された後に脆弱性の修正対応を行うようにしましょう。

脆弱性対応で慌てないために、常日頃からソフトウェア開発元、メーカーの脆弱性に関するサポート情報や、国内外の脆弱性情報に関する調整機関の発表に注意し、迅速な対応を行えるように意識しましょう。

なお、基幹業務で使用しているサーバでは、止められないなどの理由によりソフトウェアの

更新が先延ばしにされがちです。このようなサーバがサイバー攻撃を受け、長期間の業務停止や休業を強いられる可能性があるため、安易な先延ばしを行わないようにしましょう。場合によっては、更新作業が日常の業務に影響する場合も考えられますが、組織幹部の判断を仰ぐなどして対応することが必要です。

マルウェア（ウイルス等）対策管理

自分のパソコンや社内のネットワークを防御するためには、まずマルウェアへの適切な対策が必要です。最近のマルウェアは、電子メールをプレビューしたり、Web ブラウザでホームページを閲覧したりするだけで感染するなど、多様かつ巧妙なものになってきており、以前に比べて被害の内容や規模が急速に拡大してきています。

マルウェア感染の予防対策としては、まず OS やソフトウェアを更新して最新の状態に保つことが大切です。併せて、マルウェア対策ソフトをインストールした場合は、パターンファイルを常に最新のものに更新しておくことも大切です。

次に、企業や組織での情報システム部門などからのマルウェアに関する連絡に注意を払い、怪しい電子メールが届いた場合は、情報システム部門などにすぐに連絡することです。また、Web ブラウザの設定についても、適切な設定に変更することも大切です。

しかし、ここに挙げたマルウェア対策を十分に実施していたとしても感染してしまうことがあります。マルウェアは、日々新しいものが出回っており、OS のアップデートやマルウェア対策ソフトでは対応しきれないことがあるからです。

もし、マルウェアに感染してしまった場合は、パソコンの LAN ケーブルを抜く、無線 LAN のスイッチを切るなどの方法で、社内のネットワークからパソコンを切り離すことを心がけてください。ネットワークにつながったままにしていると、企業や組織全体にマルウェアを蔓延させてしまうこともあるためです。その上で社内の情報システム部門などに連絡しましょう。

■ マルウェア対策ソフトの確認

マルウェア対策ソフトがパソコンにインストールされている場合には、通常、パソコンのタスクバーと呼ばれる領域にマルウェア対策ソフトが動作していることを示すアイコンが表示されます。または、パソコンのプログラムの一覧で、マルウェア対策ソフトが含まれているかどうかを確認するという方法もあります。

自分の使用しているパソコンにマルウェア対策ソフトがインストールされていない場合には、情報管理担当者に確認してみましょう。

■　<u>パターンファイルの更新</u>

マルウェア対策ソフトが新しいマルウェアに対応するためには、常にパターンファイルを最新のものに更新しておかなければなりません。パソコンにマルウェア対策ソフトがインストールされていても、パターンファイルが古いままでは、かえって脆弱で危険な状態になりかねないので注意が必要です。(マルウェア対策ソフトの導入により、OS 自身のセキュリティ機能が無効となっている場合があるからです)。

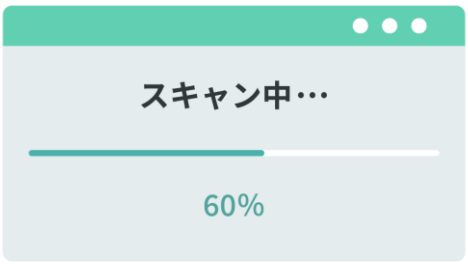
自分のパソコンのマルウェア対策ソフトがどのような契約内容になっているかということを確認し、契約が切れてしまっている場合には、新たに契約を延長するか、新規にマルウェア対策ソフトを購入しなければなりません。一般的なマルウェア対策ソフトでは、契約期間が設定されているため、パターンファイルの更新や契約方法について、確認して利用するようにしましょう。

パターンファイルは、マルウェア対策ソフトによって、マルウェア検知用データ、マルウェア定義ファイルなどの名前でも呼ばれています。

■　<u>定期的なマルウェアスキャンの実行</u>

マルウェア対策を万全にするためには、マルウェア対策ソフトを導入して、パターンファイルを更新するだけでなく、定期的なマルウェアスキャンを実行することが大切です。ほとんどのマルウェア対策ソフトでは、指定したスケジュール(毎週金曜日の夜８時など)で、システム全体に

対するマルウェアスキャンを実行することができるようになっています（ただし、その時刻にパソコンの電源が入っていない場合には実行されません）。お昼休みや定例の会議の時間など、自分の予定に合わせて、スケジュールを設定しておくとよいでしょう。



■　USB メモリを介したマルウェア感染への対策

USB メモリなど記憶媒体の自動実行機能を利用して、パソコンに差し込んだだけで感染するマルウェアも存在します。これらへの対策として、許可されていない記憶媒体や持ち主の分からないものを使用しないようにしてください。また、記憶媒体を差し込んだときには、フォルダやファイルを開く前に必ずマルウェアチェックを行うようにするとよいでしょう。パソコンの設定を変更して、自動再生機能を停止しておくと、さらに安心して利用できるようになります。

電子メールと Web サイトにおける対策

電子メールにおけるセキュリティ対策

特定の企業や組織を狙った標的型攻撃メールにより、重要な情報が盗まれる事件が頻発しています。業務関連のメールを装ったマルウェア付きメール（標的型攻撃メール）を、組織の担当者に送付する手口が知られており、従来は府省庁や大手企業が中心に狙われてきましたが、最近では地方公共団体や中小企業もそのターゲットとなっています。

標的型攻撃は、実在の人物・組織になりすますなど、狙われた組織向けに巧妙に作り込まれているため、完璧な防御対策を立てることは困難であるのが現状です。被害を最小限に抑えるためには、攻撃の侵入を防ぐための対策、侵入された場合にすばやく検知するための対策、検知した場合にすばやく対処するための対策をバランスよく行うことが重要です。以下で紹介するような、さまざまな対策を組み合わせて、多層的な対策を行うようにしましょう。

コラム：Emotet（エモテット）
近年、Emotet というマルウェアの被害が増えています。Emotet は実在する組織・人に成りすましたメールに添付されているファイルを実行することで感染します。感染した PC 内のメールソフトの過去のメール情報等を利用してなりすましたメールを送信することで感染拡大を試みるため、少しでも不自然に感じるメールには注意が必要です。

（参考）IPA「Emotet（エモテット）関連情報」
https://www.ipa.go.jp/security/emotet/index.html

■ 入口対策（攻撃の侵入を防ぐ対策）

マルウェア付きのメールを入口段階で阻止し、情報システムを保護するには、まず基本の対策としてメールのフィルタリングサービスやマルウェア対策ソフトを利用することが必要です。しかし、標的型攻撃メールに利用されるマルウェアは、市販のフィルタリングサービスやマルウェア対策ソフトなどに検知されないものも多く、それだけでは十分な対策とは言えません。

標的型攻撃に利用されるマルウェアには、実行形式（拡張子が.exe）のものや、組織でよく利用されるソフトウェアの脆弱性を突くものが多いとされています。実行形式の添付ファイルは開かないなどのルールを組織全体で徹底することや、組織で利用するソフトウェアを常に最新の状態にしておくことが重要です。

一方で、昨今、ソフトウェアの脆弱性が発見されても、修正プログラムが作成されるまでに時間を要するケースが見受けられ、その間に未修正の脆弱性を狙った攻撃が行われることがあります。これは、ゼロデイ攻撃と呼ばれ、従来の手法では対応が困難な課題として認識されています。情報管理担当者は、常日頃からソフトウェア開発元や、国内外の調整機関の発表に注意し、最新のソフトウェアの脆弱性関連情報を入手できる状態を確保しましょう。未修正の脆弱性が発表された場合は、関係機関などが公表する一時的対策を適用するなどしながら、普段以上に、攻撃に対する警戒を怠らないようにしましょう。

最近では、未知のマルウェアに対処するため、組織に送られたメールを別の安全な実行環境の中で実行してみて、そのふるまいの危険性を調べるセキュリティ製品なども提供されています。

また、こうしたシステム上の対策と同時に、後で述べる社員・職員の意識向上を通じて、不審なメールを見抜く対策も重要です。

■　出口対策（侵入後に被害の発生を防ぐ対策）

入口段階で攻撃を防げず、組織にマルウェアが侵入してしまった場合にも、組織内から重要な情報が外部に送信される段階で被害を食い止める対策（出口対策）を行うことが重要です。主な出口対策としては、マルウェア感染による外部への不審な通信を見つけて遮断する、サーバや Web アプリケーションなどのログを日常的に取得し、異常な通信を見つけるために定期的にチェックするといった対策があり、侵入の早期発見と迅速な対応のために有効です。特にログの取得は、侵入の発覚後に被害内容の特定や原因の追及をするために重要な情報源となります。

さらに、万が一データが流出してしまっても、情報にアクセスできないようデータを暗号化しておくなどの対策も重要です。

■　社員・職員へのメール訓練の実施

標的型攻撃による被害を防止するためには、メールを受信する社員・従業員への教育が欠かせません。実際に想定される標的型攻撃のメール文を見せながら、典型的な手口や、開封してしまった場合の対応などを啓発するような教育が効果的です。最近では、社員や職員に擬似的な標的型攻撃メールを送り、教育の効果測定や標的型攻撃への意識向上を図るという方法も使われています。

また、最近の標的型攻撃メールは、フリーメールアドレスを利用して送信されることが増えているので、社員・職員への注意を促すため、フリーメールアドレスからのメールには、LAN シ

ステム側でヘッダや本文に注意を促す文言を挿入してから配送する対策も考えられます。

そのほか、送信ドメイン認証（SPF）の認証結果を利用できると、正規のドメインを詐称して送信された不審メールを特定するための手がかりになります。

■ 被害に気づいたときには

上述のような多層的な対策を行ったとしても、標的型攻撃を完全に防ぐことは難しいため、実際に被害を受けた際の対応についても想定しておくことが大切です。まずは、情報セキュリティポリシーなどの中で、社員・職員が異常に気づいた際に、組織内のどの部門に連絡するかなどを事前に決め、定期的に周知するようにしましょう。次に、連絡を受けた部門でも、適切かつ迅速な処理を行えるよう、あらかじめ初動対処について対応方策を定めておき、訓練などを通して事故にそなえるようにしましょう。

感染した端末の特定や流出した情報の確認など、被害状況の把握や、再発防止策の実施にあたっては、外部の専門機関に協力を求めることが必要な場合も多くあります。そのような専門機関との連絡方法についても、事前に初動対処の一環として検討しておくようにしましょう。

【コラム】送信ドメイン認証技術

迷惑メールや不審メールの多くは、送信元メールアドレスを詐称しています。この対策として考案された技術が、送信ドメイン認証です。送信ドメイン認証は、電子メールの送信者情報のうち、ドメイン部分の正当性確認を目的としています。

送信ドメイン認証技術は、現在は主に SPF(Sender Policy Framework)と DKIM(Domain Keys Identified Mail)の 2 種類の規格が知られています。SPF は電子メールの送信元の IP アドレスをもとに、DKIM は電子署名をもとに、メール送信者情報のド

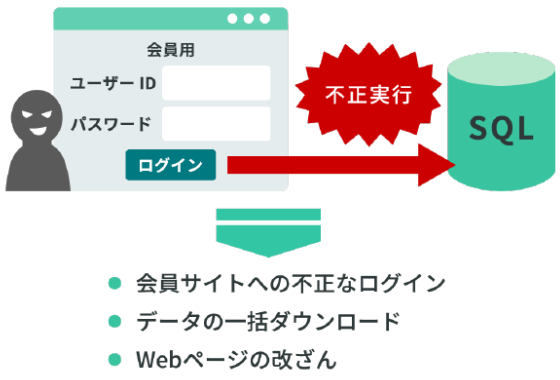
メインの正当性を評価します。この技術を導入することにより、受信者側はメールの送信者情報（From）やエンベロープ情報から送信元の正当性を確認することが可能になり、なりすましが行われた場合はそれを検出できることになります。

なお、DKIM は、署名する MTA（メール転送エージェント：Mail Transfer Agent）から検証する MTA まで、ほぼエンドツーエンドの完全性を提供します。多くの場合、署名する MTA が送信者に代わり DKIM 署名ヘッダを追加し、また検証する MTA が DNS 問い合わせにより送信者の公開鍵を入手して署名の検証を行うことで、受信者に代わって受信したメールの正当性を確認します。

ウェブサイトにおけるセキュリティ対策

多くの企業や組織のホームページやショッピングサイトは、データベースを利用した Web アプリケーションが使われています。このような場合には、Web サーバ経由でのデータベース接続を利用した攻撃方法である SQL インジェクションへの対策が必要です。

SQL インジェクションへの対策を行っていない Web サイトでは、例えばログイン画面でパスワードの欄に不正なデータベース命令を実行するための文字列を入力することで、パスワードを知らない攻撃者が正当な利用者としてログインし、クレジットカード番号などの個人情報を窃取したりすることがあります。
また、別の方法によって、データベースに保存されているデータを一括で取り出されてしまったり、データが不正に改ざんされたりすることもあります。最近は、このような手法による個人情報の漏洩（ろうえい）事件が相次いで発生しています。



また、SQL インジェクションを利用した特殊な命令によって、サーバ上のファイルを書き換えることで、Web ページが改ざんされてしまう事件も発生しています。書き換えられた Web ペ

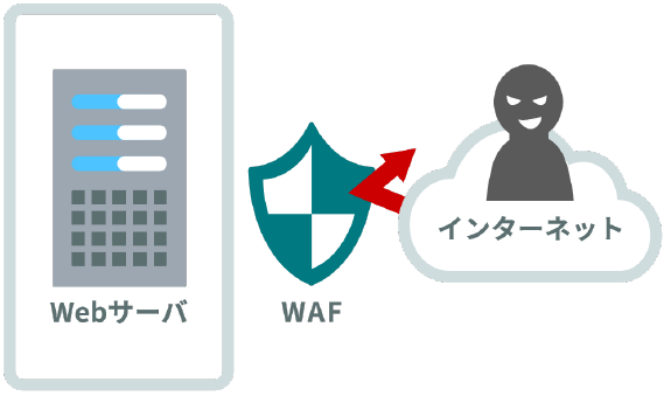
ージでは、多くの場合、訪問者には分からないような状態（表面上は正規サイトがそのまま表示される）で、利用者を悪質な Web サイトに誘導したり、iframe タグで埋め込んだ別の Web サイトからウイルスに感染させたりすることが多いようです。

自社の Web サーバでデータベースと連携したプログラムを利用している場合には、開発担当者または委託先の業者に必ず以下のような対策を講じるように依頼してください。

- Web サーバ上のプログラム（スクリプト）で SQL インジェクション対策（不正な入力値による処理を防ぐなど）を行うこと。
- Web サイトにシステムから表示されるエラーメッセージをそのまま表示しないようにすること（攻撃者に対してヒントを与えてしまうことになるため）。
- システムで利用するデータベースアカウントに対しては、最小限の権限だけを設定すること。
- 定期的にアクセスログから攻撃数を検出し、攻撃内容の解析を行うこと。
- 定期的に Web サイト全体の脆弱性（ぜいじゃくせい）検査を行うこと。

また、ウェブアプリケーションファイアウォール（WAF）を利用するのも、有効な SQL インジェクション対策となります。

WAF は、Web アプリケーションのやり取りを把握・管理することによって不正侵入を防御することのできるファイアウォールのことで、従来のファイアウォールがネットワークレベルでの管理であるのに対し、WAF は Web アプリケーションのレベルで管理を行います。WAF では、プログラムに渡される入力内容などを直接に検査することで、不正と見なされたアクセス要求を遮断することができます。Web ブラウザと Web サーバを仲介するかたちで、Web ブラウザとの直接的なやり取りを WAF が受け持つことで、SQL インジェクションなどの不正な要求に対して、「攻撃」と見なして通信を遮断することができます。



外部の業者に開発、運用を依頼している場合には、SQL インジェクションの対策状況につい

て、しっかりと確認しておくことが大切です。また、ツールを利用して外部からの侵入テスト（ペネトレーションテスト）を実施したり、専門の業者にテストや診断を依頼したりする方法もあります。

　何よりも大切なことは、常に情報セキュリティに関する情報を収集して、新しい攻撃方法が公開された場合には、利用しているサーバで必要な対策を迅速に実施することです。

脆弱性診断・ペネトレーションテスト

脆弱性診断やペネトレーションテストを実施することで、システムの持つ弱点を見つけることができます。脆弱性診断やペネトレーションテストにはいくつかの方法がありますが、もっとも確実な方法は情報セキュリティ専門家による診断サービスを依頼することです。

■ 脆弱性診断

Web アプリケーションやプラットフォームなどシステムに脆弱性を発見するために行う検査を脆弱性診断と言います。

後述のペネトレーションテストと異なり、対象のシステム全体に対して網羅的に検査を行い、攻撃のきっかけとなりうる脆弱性を見つけることを目的としています。情報セキュリティの企画や基準と照らして評価を行うため、直ちに攻撃に繋がらないがセキュリティ上望ましくない点も含めて脆弱性を洗い出すことができます。

■ ペネトレーションテスト

攻撃者と同じ視点で攻撃を行い、実際に攻撃が成功するかをリスクベースで確認する検査をペネトレーションテストと言います。

脆弱性診断と異なり、現実的に想定される攻撃シナリオに沿って目的を達成できるかを確認します。そのため、攻撃者にとって狙い目となるセキュリティ上の欠陥が無いかを評価することができ、その攻撃シナリオによってどの程度の被害が生じるかも確認することができます。

脆弱性診断やペネトレーションテストを行い、Web アプリケーションの SQL インジェクションの脆弱性や、セッションハイジャックの脆弱性の有無などを診断することで、設置したサーバのセキュリティ強度が確認でき、さらに強化すべきポイントを明確にすることができます。

なお、これらのセキュリティ診断は一般的には有料のサービスとして提供されていますが、インターネットで公開されているフリーウェアの診断ツールを入手して、自分である程度のチェックを試みる方法もあります。

セキュリティ啓発活動・教育の実施

策定した情報セキュリティポリシーを周知し、遵守してもらうために、全社員や職員に情報セキュリティ教育を実施する必要があります。

単に、分厚い資料を渡したり、形だけの方針や指針を伝えたりするだけでは、社員や職員に情報セキュリティポリシーに則って行動してもらうことはできません。

そのため、情報セキュリティに関する同意書にサインしてもらう、違反時の規定を設けるなどの方法で、情報セキュリティポリシーを意識させる仕組みが必要です。併せて、セキュリティ教育を定期的に行うことも有効です。

すべての社員や職員が遵守するからこそ、情報セキュリティポリシーが意味あるものになり、情報セキュリティ対策が効果的になります。そのような情報セキュリティに対する意識を、定期的なセキュリティ教育を通じて社員や職員一人ひとりに啓発することが、企業や組織における大切な情報セキュリティ対策の一つです。

テレワーク端末の保護

テレワーク時のルール策定

テレワークの導入等で、社員や職員にノートパソコンなどの業務用端末を自宅や外出先で利用することを許可する場合、情報管理担当者として対策を講じておかなければならないのは、機密情報や個人情報の漏洩（ろうえい）についてです。情報漏洩（ろうえい）のリスクを軽減させる対策は、職員個人では困難なことも多いため、できるだけ情報管理担当者が主体となって企業や組織全体におけるルールを決めておくべきです。

そして、情報セキュリティポリシーなどで組織全体としてのルールを明確に決めて、職員に徹底させることも大切です。たとえば、以下のようなルールを検討してください。

- 持ち出し専用の端末を別途準備し、あらかじめ UEFI やハードディスクにもパスワードを設定するなどの方法で、通常オフィスなどで利用する端末よりも強固な情報セキュリティ対策を施しておく。
- 持ち出し用端末についても、ソフトウェアの更新やウイルス対策ソフトの導入・更新などのメンテナンスを適切に行う。
- ハードディスクのデータを暗号化して利用する。
- 持ち出し用以外の端末は、原則社外への持ち出しを禁止する。
- 外部に端末を持ち出す場合には、事前の申請を義務づける。さらに、持ち出す情報の種類（個人情報、機密情報など）や内容（顧客名簿など）、目的も申請させるようにする。
- 万一、実際に事件や事故が発生した場合の対処方法や責任の所在を明確にし、申請時に確認させる。

また、パソコンの紛失や盗難によって情報漏洩（ろうえい）を引き起こさないための技術的な対策として、シンクライアントや仮想デスクトップの利用も検討しておきましょう。

シンクライアント/仮想デスクトップの利用

シンクライアントや仮想デスクトップ技術を使うことにより、社員や職員が使うパソコン本体に重要情報を保存しないようにすることができるため、紛失時などの情報漏洩（ろうえい）対策に効果的です。また、ソフトウェアをサーバ側で一元的に管理するため、更新などのメンテナンスが行き届くという点も、情報セキュリティ対策として有効です。

シンクライアントとは
ソフトウェア管理やデータ処理をサーバ側に集中させて、利用者が使う端末には必要最小限の処理をさせるシステムです。利用者の端末で処理をしているように見えますが、実際はサーバ上でデータを処理・保管しており、その画面を利用者の端末に転送して表示しているのです。

仮想デスクトップとは
　シンクライアント同じような仕組みに、仮想デスクトップがあります。仮想化技術を用いて、サーバ上で複数のデスクトップ環境を実行させる技術です。利用者はシンクライアント端末などから、ネットワーク経由で企業・組織のサーバに接続し、自分のデスクトップ画面を呼び出して利用します。

MDM（Mobile Device Management：モバイルデバイス管理）

　この他、社員・職員が業務でスマートフォンを利用する機会も増えてきました。スマートフォンは、パソコンに比べて紛失する危険性が高いため、紛失した場合のリスクに備えることがい

っそう必要になっています。

企業・組織では、MDM(Mobile Device Management:モバイルデバイス管理)というシステムを使って、スマートフォンなどの携帯情報端末を効率的に管理する仕組みを導入することも有効な手段です。一般的に MDM では、携帯情報端末のソフトウェアの更新を一元管理したり、端末で利用できる機能を制限するなどして情報セキュリティを強化しているほか、GPS 機能を使ってスマートフォンの位置を検索したり、遠隔操作で端末のロックや内部データの消去などを行うことのできる機能も提供されています。

その他、テレワークにおけるセキュリティ対策については、こちらのサイトも参考にしてください。

テレワークにおけるセキュリティ確保
(https://www.soumu.go.jp/main sosiki/cybersecurity/telework/index.html)

【コラム】UEFI のパスワードとハードディスク・SSD の暗号化

UEFI とは、Unified Extensible Firmware Interface の略で、パソコンの電源を入れたときに最初に起動するプログラムです。UEFI パスワードとは、この UEFI に対して設定できるパスワードのことで、パソコンの起動にパスワードが要求されます。パソコンにログインするためのパスワードとは別にパスワードが必要になるため、パソコンに不正にログインされる危険性を減らすことができます。ただし、UEFI のパスワードを忘れてしまった場合には、パソコンの製造元に依頼しなければ解除できないという問題もあるため、注意が必要です。

ハードディスク・SSD の暗号化は、パソコンに内蔵されているハードディスク・SSD 上のデータを暗号化する機能です。ハードディスク・SSD の暗号化を設定してしまえば、パソコンが分解されてハードディスク・SSD を抜き取られてしまっても、他のパソコンでデータを読み取ることは困難になります。

これを採用した場合、将来ハードディスク・SSD を廃棄する際に、暗号化消去(後述)が利用できるようになります。

なお、UEFI のパスワードとハードディスク・SSD の暗号化については、使用するパソコンによって装備されていなかったり、機能が異なったりすることがありますので、パソコンの説明書やメーカーのホームページなどで確認してください。

アカウント管理

攻撃者は、正規のユーザーの ID およびパスワードを用いて組織の機密情報等に不正アクセスを行うことがあります。
正規のユーザ情報を入手される原因としては以下のようなことが挙げられます。

- 脆弱なパスワードの利用
- 漏洩したオンラインアカウントで使用しているパスワードと同じパスワードの利用
- 退職したユーザのアカウントを利用
- テストアカウントの利用
- 長期間変更されていない共有アカウントの利用
- ソーシャルエンジニアリング

■ 安全なパスワードの設定・管理

一般従業員より、システム管理者の方がより多くの権限を保有しているため、システム管理者のアカウントやシステムの特権を有するアカウントは格好の標的になります。
推測されやすいパスワードを設定しない様に、システムを利用する人（従業員）に対して以下の内容をアナウンスする様にしましょう。またシステム管理者のパスワードについても同様の対策を講じるようにしましょう。

従業員からパスワードの再発行依頼があったときには、利用者の本人性の確認が必要になります。電話での問い合わせに対し本人確認をせずに、電話で回答するというのではソーシャルエンジニアリングの危険があります。本人確認の方法として、問い合わせた本人が所有していることがわかっている電話にコールバックを行うことや、本人しか知り得ない情報を確認するなど、あらかじめ適切な対応方法を決めておきましょう。

■ アカウントの棚卸

長期間利用されていないアカウントや、本来であれば削除しておくべきアカウントがないか定期的に確認し、不要なアカウントは無効化したり、削除するようにしましょう。

コラム：ソーシャルエンジニアリングとは

ネットワークに侵入するために必要となるパスワードなどの重要な情報を、情報通信技術を使用せずに盗み出す方法です。その多くは人間の心理的な隙や行動のミスにつけ込むものです。

具体的な手口：

- システム管理者になりすまして電話でパスワードを聞き出す
- 肩越しにキーボードでの入力を見る（ショルダハッキング）
- ごみ箱を漁り、有益な情報を探しだす（トラッシング）

ごみ箱の紙くずから情報を探し出す

アクセス制御・管理

社内ネットワークに対する情報セキュリティ管理のためには、個々の利用者ごとに適切な権限を設定する必要があります。利用者に与える権限は、すべての利用者にすべての権限を与えるのではなく、最低限必要な利用者にのみ必要最低限のアクセスを許可することが大切です。

■　職務や役割によって最小限の権限を付与する

部門ごとでのアクセス制御の例では、開発中の製品のデータが格納されているファイルへのアクセス権限を開発部門には付与して、営業部門には付与しないということも考えられます。あるいは、編集・削除・閲覧権限を開発部門には付与するが、営業部門には、閲覧の権限のみを付与するといった権限の付与の仕方もあると思います。

■　アクセス権の確認

人事異動や、退職、新入社員の受け入れ等で、組織の人員構成に変更があった際には都度アクセス権設定の見直しを実施し、本来はアクセスすべきでない人が特定の情報にアクセスできることがないようにすることが重要です。

また、定期的にアクセス権の棚卸を実施し、一時的に利用したテストユーザや、一時的に特定のユーザに付与した権限が残っていないか、退職したユーザが有効になっていないか等の見直しを行うことも重要です。

監査ログの管理

外部からの不正アクセスやウイルス感染により、組織内部からの情報漏洩等の事故が発生してしまった場合、そのことにいち早く気づき、被害状況や影響範囲の調査などの事後対応を効果的に行うためには、監査ログ（通信記録）の取得と保管が重要になります。

そのときネットワークでどのような通信が行われていたか、情報システム内で何が起こっていたかなど、後から追跡調査を行う際に監査ログの解析が役立ち、事故の原因究明や、事後の抜本的な対策を導き出すことにつながります。

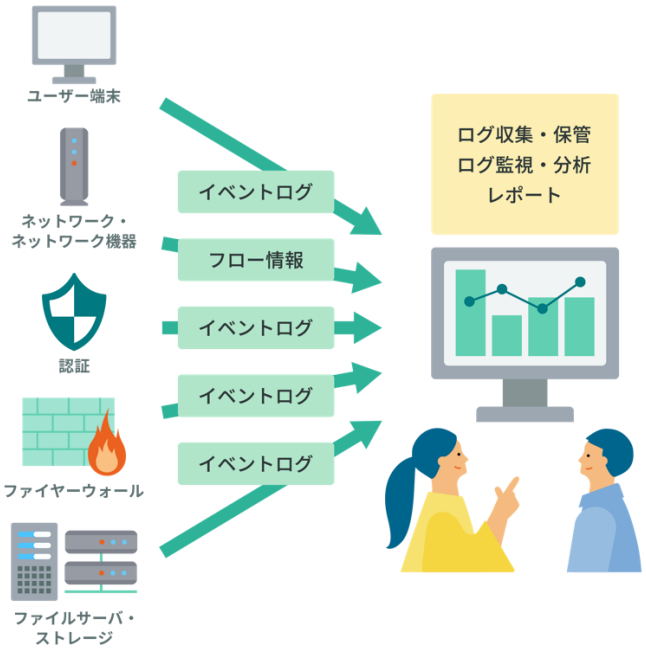
■ 監査ログの種類と内容

監査ログの具体的な例としては次のものが挙げられます。

- ファイアウォールを通過した通信、または拒否された通信のログ
- 侵入検知システム（IDS）や侵入防止システム（IPS）が監視した通信のログ
- DHCP サーバがパソコンに IP アドレスを割り当てたログ
- ファイルサーバへのアクセスのログ
- ファイルの参照や、編集などの成功や失敗のログ
- 情報システムへのログイン、ログアウトなど認証の成功や失敗のログ
- Web サーバへのアクセスのログ
- Web サーバが利用者から受け取った入力内容のログ
- Web プロキシサーバが中継した通信のログ
- データベースサーバへのアクセスのログ
- アプリケーションが出力する処理結果の正常終了、異常終了などのログ
- パソコンの操作ログ

それぞれのサーバやシステムが出力するログの内容は、通信やアクセスの送信元・送信先の IP アドレスを始めとして、通信に使用されるポート番号、命令の内容、通信データ自身など、さまざまなレベルがあります。出力されるログの詳細度は一般的には設定によって制御できますが、どのような内容のログを取得するべきか、またその保存期間をどの程度とするかは、組織が扱うデータの性質や、システムの処理能力、ネットワーク構成などに大きく関係します。さらに、組織が受ける可能性があるネットワーク攻撃を事前に想定し、それを考慮したログの取得・管理方法を設計に反映することで、調査が必要になった場合に、より役に立つ情報を得られることが考えられます。

必要な監査ログの種類と内容について、組織内で十分に検討を行い、適切な監査ログを取得できるようにしましょう。



■　システムの時刻同期の必要性

ログを取得する場合、各コンピュータ間でシステムの時刻を一致させておく必要があります。この時刻の同期が不適切であると、ログに記録された時刻がずれてしまい、各システム間でログを相関的に分析することが困難になります。

システムの時刻を同期させる手段として、一般的に NTP(Network Time Protocol)が広く利用されています。実際に NTP が正しく設定され、正常に動作していることを確認しておくことが重要です。

■　ログの保管とバックアップ

ログは、収集した機器の本体内ではなく、ログ取得のために別途ログ管理システムなどを設計し、そこで保管を行うことが推奨されます。そうすることで、ログの改ざんなどの不正行為からの保護だけでなく、ログ解析プログラムによる可視化処理を行ったり、保存期間の制御なども行いやすくなります。

また、一定期間を経過したログの保管方法として、コストや保存期間を考慮し、外部記憶媒体等に保管する運用も検討しましょう。通常のデータのバックアップと同様に、ログのバックアップも重要になります。

■　ログの取り扱いの注意

ログには、誰と誰がいつどのような内容の通信を行ったか、という情報が記録されています。また、企業秘密に関する情報や、電子メールの内容、利用者が入力した個人情報などがそのまま含まれている場合もあります。ログは機密情報であるということを理解し、取り扱いには十分な注意が必要です。

例えば、外部のセキュリティ調査会社にログを開示して調査を依頼する際には、ログの内容に関して秘密保持契約を結んだり、ログを外部に持ち出さなければならない際にはデータの暗号化を検討するなど、秘密の保全に関する対応が必要であることを理解しましょう。

データ復旧・バックアップの管理

企業や組織内の情報資産に対する可用性を維持するためには、保有している情報に対する適切なバックアップが必要です。情報管理担当者には、ランサムウェアへの感染、パソコンやネットワークの障害、システムの操作ミスなどが発生した場合にも業務にできる限り影響を与えない、迅速に復旧可能なバックアップの運用が要求されています。

企業や組織内の利用者が安全にパソコンを利用できるようにするには、定期的なバックアップを推奨しなければなりません。業務で通常使用するパソコンでは、ワープロソフトや表計算ソフトなどで作成したドキュメントファイルだけでなく、電子メール、よく利用するホームページのURL、各種の設定などもバックアップさせる対象としておきましょう。

まず、情報セキュリティポリシーにバックアップの方法や頻度を組織内のルールとして、明確に記載しておきましょう。

なお、バックアップの方法や保管場所等については、トラブル発生時に復旧できることが重要です。ポリシー策定の際に留意する必要があります。

例えば、ランサムウェアに感染してしまい、パソコンやサーバ内のデータが暗号化されてしまうなどの事態がありえます。

サイバー攻撃、災害等何がおきても、どれかひとつは残るようにするという考え方が重要です。

具体的なバックアップ方法の対策例として以下が挙げられます。

■　物理的な隔離

オフラインバックアップであれば、バックアップ媒体を遠隔地に輸送して保管する。オンラインバックアップでは遠隔地にあるストレージにバックアップを実施する。これらの方法は特に災害リスクへの対策となります。

■　自動暗号化保存

バックアップ先にクラウドサービスを利用する場合に、バックアップ先からの情報漏洩リスクを防ぎます。復号化に必要な鍵は安全に保管する必要があるのはもちろんです。

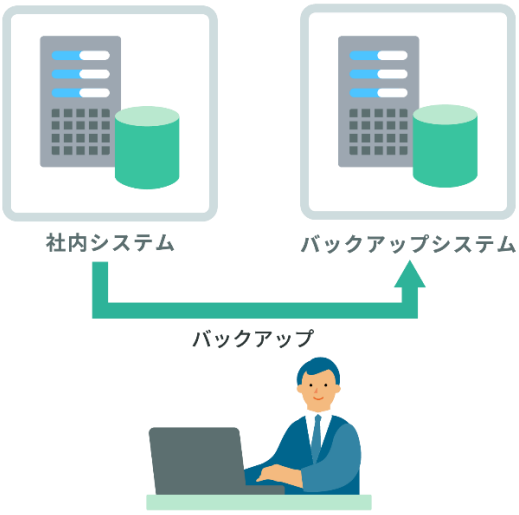
■　ネットワーク上の隔離

オンラインでバックアップを実施する場合は、サイバー攻撃リスクを考慮して、バックアップ先はネットワーク的に分離できることが重要です。安易に同一ネットワーク上にバックアップシス

テムを接続すると、共倒れのリスクが高まります。

これら以外の対策も含めて、企業・組織の実情に応じて複数のバックアップ手段を組み合わせて、リスク低減を図ることが重要です。

また、平時からバックアップを戻す訓練を実施しておくことも推奨されます。



■　サーバ上のデータのバックアップ

データベースサーバやファイルサーバに保存されている共有データは、情報管理担当者が責任を持ってバックアップしなければなりません。

バックアップを実行するためには、OS に装備されているバックアップユーティリティや専用のバックアップソフトを利用します。なお、サーバのバックアップは、OS やバックアップソフトの持つスケジューリング機能を利用して、利用者が操作を行わない深夜や早朝などに実施します。

■　バックアップの指示

社員や職員が各クライアントに保存しているデータも、大切な情報資産のひとつです。そのため、組織内の利用者に対しても、各クライアントに保存されている情報のバックアップを指示しなければなりません。その際には、バックアップの保存先（メディアやバックアップサーバなど）、使用するバックアップソフトや方法、バックアップの頻度など、各利用者の持つ情報資産の重要度をきちんと把握して、適切なアドバイスや方法を具体的に行う必要があります。

利用者がバックアップに外部記憶媒体を使用する場合には、データの持ち出しによる機密情報や個人情報の漏洩（ろうえい）が発生する可能性が高くなるという点に注意してください。バックアップにおいて、外部記憶媒体を推奨する場合には、情報セキュリティポリシーなどで、

不要な持ち出しを禁止したり、保管場所を規定したりといった情報管理上のルールを徹底することも重要です。

■　クラウドサービスの利用

近年、インターネット上のリソースをサブスクリプションで利用できるクラウドサービスが人気です。クラウドサービスではコストと性能のバランスを取りやすいなどのメリットがありますが、サーバの運用管理を全て委託することになるため、障害時の復旧やデータのバックアップを意識する必要があります。

クラウドサービスの事業者側での障害や運用の不備などが原因で、システム上に置いたデータが消えてしまったり、サービス自体が使えなくなってしまったりという事態が発生する可能性があるため、信頼できる事業者が提供するクラウドサービスを選択しましょう。

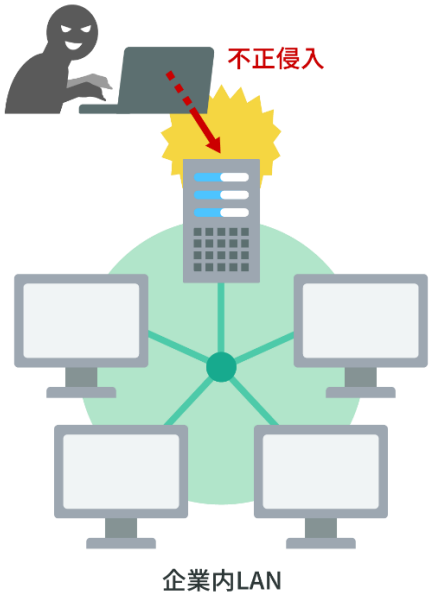
万が一、クラウドサービスで障害が発生し、データが消えてしまった場合のことも想定し、データのバックアップを取得しておく必要があります。また、サービスが使えなくなった時のために、代替の手段やサービスを用意しておくことも検討する必要があります。

インシデントレスポンス体制整備

情報セキュリティに関わる事故やトラブルが発生した場合には、情報セキュリティポリシーに記載されている対応方法に則して、適切かつ迅速な処理を行うことこそが、被害や損失を最小限に抑える最大の対策です。

昨今では BCP(事業継続計画)を策定することも多いですが、その観点で事故やトラブルの対応方法を策定しておくことも有効です。

事故やトラブルが発生した場合には、以下の手順で対応します。ここでは、ネットワークへの不正侵入を例として取り上げます。



(1) 事故の検知

定期的なログチェックや障害検知ツールの利用によって、不審な状況の発生を検知する。また、社内外からの通報窓口の整備も有効。外部でないと分からないインシデントもあるため、社外との窓口が有効だが、通報用メールアドレスを設置していても適切な担当に届かないケースもある。また、電話での通報は代表電話にかかってくることがほとんどであるため社内での連携体制を整えておく必要がある。

(2) 事故の初動処理

関連する部署や担当者へ連絡を行い、あらかじめ設定しておいた優先順位に従って手続きを行う。情報が漏洩(ろうえい)しているなどの可能性があれば、この段階でホームペー

ジを閉鎖する、データをインターネットに接続されていないパソコンに退避させるなどの処置が必要である。なお、利用者に被害が及ぶ可能性がある場合には、速やかに利用者に連絡を行う。
また、この段階でセキュリティ対策機関等への情報提供も強く望まれる（情報提供先はリンク集に記載）。早期の情報提供により、同様のサイバー攻撃の被害を防げた例もある。取引先などの関係先にも情報提供を行うことが望まれる。

（3）事故の分析
被害内容や事故の規模を整理して、事故が発生した原因を分析し、対応策を決定する。

（4）復旧作業
システムを復旧させ、正常に動作していることを確認する。復旧が完了したら、関係者や利用者への連絡を行う。

（5）再発防止策の実施
原因を究明して、同様の事故が再発しないように対策を講じる。事故に対する処理や対策で必要な項目を、情報セキュリティポリシーに反映する。

これらの一連の処理の中でもっとも重要なことは、状況を正確に判断するための情報伝達の手順やルールを確立しておくことです。過去に発生した情報漏洩事件などでは、組織幹部への情報伝達が遅れたり、正確な情報が伝わらなかったりしたために、もっとも重要な初動処理にミスが発生し、事故の被害を拡大させたケースが数多く見受けられます。

これらの情報セキュリティに関する事故の事例を参考にして、情報伝達や対応方法を手順やルールとして情報セキュリティポリシーに組み込んでおくことで、情報セキュリティ対策をさらに強化することができます。

しかし、実際にトラブルが発生した場合は、事前に策定した手順通りにはいかないことも多々あります。その際は、経営層に判断を求める必要がある場合もあります。一例を挙げれば、復旧のために通常業務をいつまで、どの範囲まで止めるのかといった判断があります。さらに例を挙げれば、ランサムウェアの被害に遭った際、通常は支払うものではないとされる身代金について、人命がかかっている等の緊急時には敢えて支払う判断もあり得ます。

これらの判断は、情報セキュリティ担当部署や担当者のみで判断できるものではないため、経営側に判断を下してもらう必要があることを意識しておかなくてはなりません。