技術的安全管理措置

目的

技術的安全管理措置は、以下の点を目的として対処をするものです。

- システムへの不正アクセスによる情報漏えいの防止
- インターネット利用における情報漏えいの防止
- 通信時における情報漏えいの防止

本項では、目的ごとに、概要、求められる要件と手法をご紹介します。

1 システムへの不正アクセスによる情報漏えいの防止

家族みんなが使うPCを仕事でも使用していて、アカウントが1つしか存在しないとします。この場合、家族みんなが仕事の資料にアクセスでき、間違って大事な資料を消したり、資料をメールで送信したりするかもしれませんので、大事な資料にアクセスできないようにしたいところです。このためには、PCの共用をやめたり、PCのアカウントを家族ごとに設定したりする必要があります。また、どちらの手法をとる場合でも、パスワードの入力が必要な状態にしておくことが必要です。たとえPCの共用をやめても、電源を入れただけで利用できる状態になるのであれば、大事な資料にアクセスされる可能性があるからです。これがシステムへの不正アクセスによる情報漏えいの防止です。

例を加えます。

PCを共用で利用し続けることに決定し、家族それぞれのアカウントとパスワードを設定することにしたとします。これで安心でしょうか。大事な資料は、共用のPCに入っています。家族全員がPCの管理者権限を持っている場合は、どのフォルダにもアクセスできますので、大事な資料にアクセスされる可能性は残っていますし、ソフトウェアをインストールしたり、PCを再度セットアップしたりすることもできますので安心とは言えません。大事な資料を守るためには、アカウントとパスワードの設定だけではなく、例えば、子供が利用する、子供の友人が利用する可能性がある等の場合も想定して、アカウントの権限を設定することも必要になるのです。

システムへの不正アクセスの防止では、リスクを低減するため、以下の2点の要件を満たす対処をする必要があります。

- 認証の仕組み（アクセス制御）を実装する
- システムの利用者の権限を管理する方法（アカウント管理）を整備する

求められる要件と手法

1 認証の仕組み（アクセス制御）を実装する

この要件は、システムを利用することができる権限を持つ人だけが利用できる状態にすることで、不正なアクセスを防止できるようにするためのものです。
認証の仕組み（アクセス制御）とは、「ID」と「個人が知っていること、または個人が所有しているもの」とを組み合わせることで、許可された利用者本人であるか否かを確認する仕組みです。「個人が知っていること、または、個人が所有しているもの」には、パスワード、ICカード、指紋、光彩などがあります。様々な認証の方法がありますが、この要件で重要なのは、制御する仕組みが機能することです。指紋認証の仕組み、光彩認証の仕組みは必須ではありませんので、費用や運用の簡易さなどを勘案して手法を選定してください。
対処の手法と取得できる記録をご紹介します。

手法の例	取得できる記録の例
個人情報を操作するソフトウェアに認証の仕組みを導入する - パスワード認証 - ICカード認証 - 生体認証 - ワンタイムパスワード認証　など	認証ログ 操作ログ
ネットワークに対して認証の仕組みを導入する - ドメインのユーザ管理の利用 - MACアドレス認証 - 不正接続防止ソフトの利用　など	認証ログ
ファイルサーバ、個々のPCに対して認証の仕組みを導入する - パスワード認証 - ICカード認証 - 生体認証 - ワンタイムパスワード認証　など	認証ログ

認証の仕組みを実装する対象には、個人情報を取り扱うソフトウェア、事務所内のネットワーク、ファイルサーバや個々のPCなどが挙げられます。これらすべてに認証の仕組みの実装を検討することが理想ではありますが、個人情報への不正なアクセスを防止することが目的ですので、個人情報を操作するソフトウェアやファイルサーバなどに対して実装することを優先してください。ソフトウェアの選定にあたっては、個人毎にアカウント、パスワードを払い出すことができる、アカウント毎の利用権限を設定できる、等の仕組みが

実装されていること確認してください。
取得できる記録（ログ）は、システムによって異なりますが、システムにログインする際の認証のログと、個人情報を操作したときのログを取得できるようにすることをお勧めします。

なお、パスワードを使用する場合には、容易に推測できたり、利用されたりすることを防ぐために、以下のパスワードルールを設定して、運用することが望まれます。

- パスワード文字列の長さ（7文字以上）
- 含まれる文字種類（英語大文字/小文字、数字、記号の混合など）
- 有効期限を設定（90日以内）
- 管理者から払い出された初期パスワードを変更すること
- パスワードを忘れた際に管理者から払い出されるリセットパスワードを変更すること

不正操作の防止として、一定時間PCを操作しない場合には、スクリーンセーバが起動し、解除する際には、パスワードの入力が求められるように設定することも有効です。

2 システムの利用者の権限を管理する方法（アカウント管理）を整備する

この要件は、システムの利用者個人と利用権限を管理し、意図しない情報の閲覧、変更、削除、毀損などを防止できるようにするためのものです。
誰が、どんな権限を持つか、という点を管理するために、特に従業者の多い事務所では、管理簿などでアクセス権限を管理することが必要になるでしょう。管理簿を作成する場合は、従業者の配属や異動等を反映するとともに、定期的に棚卸を実施し、管理簿を維持してください。
対処の手法と取得できる記録をご紹介します。

手法の例	取得できる記録の例
アカウント管理簿を整備して、個人に付与する権限を把握する	アカウント管理簿

2 インターネット利用における情報漏えいの防止

インターネットを利用する場合、常にウイルスに感染するリスクにさらされています。企業の88.6%がPC等の端末にウイルス対策プログラムを導入している（出典：平成27年度版　情報通信白書）という調査結果もありますので、ウイルス対策ソフトを導入する必要があることは理解いただけるでしょう。しかし、ウイルス対策ソフトを導入しても安心はできません。ウイルス対策ソフトは、病気のワクチンと同様で、あくまでも一部の悪意のあるソフトウェア（マルウェア）に対する対策であり、すべての悪意のあるソフトウェア（マルウェア）を駆除することができるものではないからです。

悪意のあるソフトウェア（マルウェア）はインターネットでWebサイトを閲覧している際に、システムの脆弱性を利用して感染することが多いため、セキュリティパッチを適用して、システムに脆弱性がない状態を維持したり、危ないWebサイトの閲覧を避けたりすることが重要です。

また、インターネットに接続している場合、インターネット上から不正アクセス攻撃を受けることもあります。自分の事務所は狙われるような大企業ではないため、不正アクセスなんて関係ない、と思っていないでしょうか。インターネットの向こう側にいる攻撃者からの攻撃は無差別であり、規模の大小は関係ないということを認識してください。

インターネット利用における情報漏えいの防止では、リスクを低減するため、以下の2点の対処をする必要があります。

- インターネットからの不正アクセスを防止する仕組みを整備する
- 悪意のあるソフトウェアの感染を防止する仕組みを整備する

求められる要件と手法

1 インターネットからの不正アクセスを防止する仕組みを整備する

この要件は、インターネットに接続しているシステムやネットワークが、外部から攻撃を受けることを防止できるようにするためのものです。

インターネットに接続している以上は、常に攻撃を受け続けていると言えますので、攻撃を防止したり、攻撃を成立し難くしたりするための対処をする必要があります。事務所内でWebサーバを持っていたり、外部から接続できる状態にしていたりする場合は必須だと考えてください。

導入にあたって専門的な知識が要求される手法もありますので、まずは、身の回りの機器、またはOSの機能を活用することによって実現できる手法を検討し、実装することが望ましいでしょう。

対処の手法と取得できる記録をご紹介します。

手法の例	取得できる記録の例
ファイアウォールの導入	通信の記録
OSのファイアウォール機能による制御	-
ブロードバンドルータによる接続先の制御	通信の記録
UTM（統合脅威管理）による制御	通信の記録

2 悪意のあるソフトウェアの感染を防止する仕組みを整備する

この要件は、ウイルスやワームといったPCを壊したり、情報を盗んだりするソフトウェアの感染を防止できるようにするためのものです。
ウイルス対策ソフトは、インターネットに接続しているPCには、比較的導入されているでしょう。しかし、前述したように、ウイルス対策ソフトだけでは防ぐことができない悪意のあるソフトウェアが存在しますので、ウイルス対策ソフトの導入に加えて、その他の手法を導入する必要があると考えてください。
対処の手法と取得できる記録をご紹介します。

手法の例	取得できる記録の例
不正なWebサイト（怪しいWebサイト）へのアクセスを制限する	Webサイトのアクセスログ
許可されたソフトウェアのみを利用する	ソフトウェア一覧
OSやソフトウェアのセキュリティパッチを適用する	セキュリティパッチ適用記録
不審な宛先からのメール、および添付ファイルを開かないようにする	-

取得する記録が個々のPCの中に保存されるものが多いため、記録を集約したり、サーバで保管したりすることが難しいと考えます。定期的なチェックを実施する際に、個々のPCの記録を確認することをお勧めします。

3 通信時における情報漏えいの防止

重要書類や貴重品を誰かに送る場合を考えましょう。郵便ポストに入れた場合、間違ってほかの人に届いてしまったり、途中で紛失して誰かに取られたりするリスクがあるので、書留や宅配便などを使って直接宛先の人に手渡しされるように、そして、配達されたことが確認できるようにするでしょう。送付しようとしているものが重要なものであれば、日常的に実施されていると思います。通信を利用した情報交換（電子メールやインターネットのサービスを利用した情報交換）においても同様に、宛先の確認や到達確認を行う必要があります。これが通信時における情報漏えいの防止です。

次に、電子メールで情報を送信する場合を考えましょう。誤送信の予防として、宛先をチェックすることは当然に必要になります。しかし、宛先を人間が入力する以上は、誤送信を完全に防ぐことできません。そのため、万が一誤って情報を送信してしまった場合に備えて、情報の中身を見ることができないようにすること、利用することができないようにすることも必要になります。

「通信時における情報漏えいの防止」は、基本的に電子情報を対象としていますが、実務において、FAXを使用して外部に送信することがあることから、FAXも含めて記載します。

「通信時における情報漏えいの防止」では、リスクを低減するため、以下の3点の対処をする必要があります。

- 電子メールでの情報送信時に情報が漏えいしない仕組みを導入する
- インターネットのサービスを利用した情報送信時に情報が漏えいしない仕組みを導入する
- FAXを利用した情報送信時に情報が漏えいしない仕組みを導入する

求められる要件と手法の例

1 電子メールでの情報送信時に情報が漏えいしない仕組みを整備する

この要件は、情報を電子メールで送信する際に、誤送信をしてしまった場合や盗聴された場合でも情報の中身を簡単にみることができないようにするためのものです。
電子メールの宛先間違いを避けるために、ダブルチェックをすることは当然に必要になりますが、その場合でも、万が一に備えて、必ず情報にパスワードをかけるようにすることをお勧めします。
対処の手法と取得できる記録をご紹介します。

手法の例	取得できる記録の例
宛先を再確認する	送受信ログ
添付ファイルにパスワードを設定、もしくは暗号化する （パスワードは別途相手に伝えること）	
誤送信対策ソフトを利用する	

メールの送受信ログ（少なくとも送信ログ）を取得し、保管することをお勧めします。

2 インターネットのサービスを利用した情報送信時に情報が漏えいしない仕組みを整備する

この要件は、電子メールと同様に、情報をインターネットのサービスを利用して送信する際に、誤送信をしてしまった場合や盗聴された場合でも情報の中身を簡単にみることができないようにするためのものです。
インターネットのサービスを利用する場合には情報が保存され続ける可能性がありますので、サービス上に保存されている情報を削除することが必要です。
対処の手法と取得できる記録をご紹介します。

手法の例	取得できる記録の例
宛先を再確認する	送受信ログ 利用ログ
添付ファイルにパスワードを設定もしくは暗号化する (パスワードは別途相手に伝えること)	
送信後にインターネットのサービス上に残っている情報を削除する	

利用するインターネットサービスが安全である必要があるため、サービス提供者の情報を確認し、インターネットのサービスへのアクセスが暗号化（https）されている、または接続するにはクライアント証明書が必要となっている等のサービスを選定してください。

3 FAXを利用した情報送信時に情報が漏えいしない仕組みを整備する

FAX送信では、宛先確認と送付後の原本管理の2点に注意をする必要があります。
例えば誤送信を避けるため、送信前に宛先のダブルチェックを行うこと、送信後に受信者に対して電話などで受領確認を行うことが挙げられます。
FAXは紙の資料を利用しますので、送信後に紙資料が放置状態にならないように、原本資料を回収し、保管ルールに従って保管してください。
なお、実施した記録を取得することが難しいため、運用をチェックする際には、ヒアリングや目視確認などを実施するようにしてください。