7 アクセス制御

ID・パスワード

ネットワークや情報システムにアクセス制御するために、ID・パスワード管理は重要です。「パスワードのずさんな管理」や「類推されやすいパスワードの使用」は、「不正アクセスの脅威」に直結することから、絶対に避けるべきです。情報システムの管理者は、次のようなことを参考に、利用者に対し、適切なパスワード設定について周知することが必要です。

最近ではパスワード認証に代わって、より強固なユーザの生体特性を利用した生体認証システムも広く用いられるようになりました。

［適切なパスワード設定の例］

- ■最低8文字以上にする（一般に長いほど安全）
- ■大文字、小文字、数字や記号を混在させる
- ■簡単に類推できるもの（氏名、誕生日、辞書にある単語など）は使わない
- ■パスワードを記載したメモなどを適切に管理し、他人の目に触れないようにする
- ■定期的に更新し、再利用しないようにする
- ■一定回数以上ログインに失敗したユーザIDは理由が特定できるまで利用停止とする

アカウント管理

アクセス制御を適切に実施するには、利用者のID・パスワードを適切にし、退職者、テスト用等の必要のないID・パスワードを確実に失効させる必要があります。アカウント管理が不十分で、退職者が当時のID・パスワードを利用して不正アクセスする事件が発生しており注意が必要です。また、システムなどに大きな権限がある管理者のパスワードはより厳格な管理が要求されます。

他人のID・パスワードを奪取・盗用し、その者になりすましてシステムにアクセスする行為は、「不正アクセス禁止法」に違反し、犯罪になります。

8 暗号

機密性の高い情報の保管時や、インターネット等を利用したリモートアクセス環境による通信、情報交換においても、セキュリティを高めるために暗号化を行うことをお勧めします。

電子署名

暗号技術を活用した電子署名による認証は、電子文書の偽造、改ざんを防止します。電子署名は、文書の電子化が進む中、紙文書における印影やサインに相当する機能として注目されています。

電子署名及び認証業務に関する法律が平成13年（2001年）4月1日から施行され、電子署名が手書きの署名や押印と同等に通用する法的基盤も整備されました。

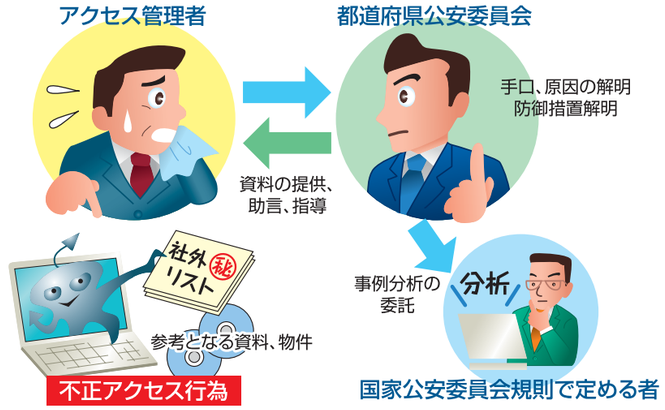
9 ログ収集と解析

- ■情報流出には内部からの流出も大きな原因となっています。利用者が情報に対しどのような操作を行っているかを正確に把握するために、ログの収集と解析が重要です。サーバやファイルにアクセスしたという記録に留まらず、書き込みを加えた、印刷をした、ダウンロードしたなど利用者の操作状況を把握するためのログ収集は有用です。
- ■ログは、事件・事故が起きた場合、原因究明のための重要な証拠になります。適切に管理しましょう。
- ■収集したログを解析することは、問題点の早期発見や内部統制活動の評価につながります。少なくとも、重要度の高い情報やそれを扱う利用者の利用状況を把握するための解析は行うようにしましょう。
- ■いつ、誰が、どこから、何に対して、何をしたのかが特定できるだけのデータは最低限必要です。しかし、あまり詳細に記録するとデータ量が膨大になるなど、かえって解析が困難になる場合があります。
- ■被害の届出先
  都道府県警察本部のサイバー犯罪に関する相談窓口
  サイバー犯罪の被害に遭った場合、遭いそうになった場合の相談及びサイバー犯罪に関する情報提供を受け付けています。（連絡先は、最終ページに記載しています。）

サイバー犯罪への警察の取組み

不正アクセス行為の再発防止のための援助措置

都道府県公安委員会は、不正アクセス行為が行われたと認められる場合において、不正アクセス行為が行われた特定電子計算機のアクセス管理者から援助を受けたい旨の申出があり、その申出を相当と認める時は、申出者に対して不正アクセス行為の再発防止のための援助措置を行います（不正アクセス禁止法第6条に規定）。具体的には、被害の再発防止のために必要な資料の提供、助言、指導等を行います。



援助の受託を申し出る場合は、サーバの設置場所を管轄する都道府県警察のサイバー犯罪相談窓口に相談を！

あなたの会社はどこまで情報セキュリティ対策が進んでいますか？

チェック欄

- ☐ 1 情報セキュリティポリシーや手順を策定し、周知徹底をしている
- ☐ 2 情報セキュリティ責任者を任命し、管理者・社員の情報セキュリティにおける役割と責任を明確にしている
- ☐ 3 法令や規定を理解し、遵守させている
- ☐ 4 情報セキュリティについて、責任者・利用者の職務や能力に応じた教育を定期的に行っている
- ☐ 5 セキュリティレベルの違いに応じて物理的なセキュリティ境界を設け、入退室等の管理を行っている
- ☐ 6 パソコンや記録媒体の持ち出し及び持ち込みに関する規定を定め、許可（承認）する場合、その記録を取っている
- ☐ 7 コンピュータをはじめとする記録媒体を内蔵した装置の廃棄や再利用に際しては、情報漏えいを防ぐため、データが確実に消去される方法を用いている
- ☐ 8 情報処理などを外部委託する場合、情報セキュリティに関する契約を締結し、適切に監督している
- ☐ 9 システム障害などによるデータ損失時等に速やかに復旧するために、データのバックアップを定期的に行うとともに、採取したバックアップデータを用いて復旧のテストを行っている
- ☐ 10 悪意のあるソフトウェアによる被害を未然に防ぐため、常に情報セキュリティにかかわる情報の収集に心がけ、適切な対策を講じている
- ☐ 11 インターネット接続に際し、社内ネットワークの安全を確保する対策を行っている
- ☐ 12 ID・パスワードを適切に管理し、社内ネットワークや重要な情報を保護するためにアクセス制御を行っている
- ☐ 13 暗号化により、機密性の高い情報を保護している
- ☐ 14 システムの利用状況等を示す情報（ログ）は重要な証拠となることを認識し、適切に収集・保全管理を行うとともに、必要に応じ解析を行っている