情報セキュリティ研修

日本赤十字社における情報セキュリティについて

日本赤十字社
Japanese Red Cross Society

総務局　財政部
情報セキュリティ対策本部

目次

出典： 総務省『国民のための情報セキュリティサイト』を加工して作成
http://www.soumu.go.jp/main_sosiki/joho_tsusin/security/

日本赤十字社
Japanese Red Cross Society

本研修の目的

本研修では、
コンピュータやインターネットについて基礎的な知識を身に付け、
情報セキュリティに関する適切な考え方や対策を習得しましょう。

犯罪者からの攻撃を未然に防ぐため

職員のセキュリティ意識を向上させるため

情報セキュリティについて見識を高めることが大切です。

日本赤十字社
Japanese Red Cross Society

情報セキュリティ対策とは

進歩したインターネット技術を悪用した

- コンピュータウイルス
- 迷惑メール
- コンピュータへの不正侵入

また、人為的なミスによる

- 個人情報の流出

などの危険から、安心してコンピューターやインターネットを使い続けられるように必要なセキュリティ対策をすること。

それが、**情報セキュリティ対策**です。

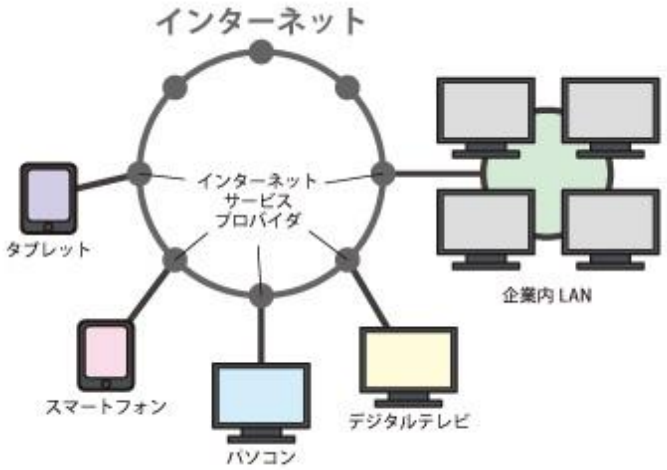
日本赤十字社
Japanese Red Cross Society

基礎知識１　インターネットとは

インターネットとは

　複数のコンピュータを、ケーブルや無線などを使ってつなぎ、お互いに情報をやりとりできるようにした仕組みをネットワークと呼びます。

　インターネットは、世界規模でコンピュータ同士を接続した、**最も大きいネットワーク**といえます。

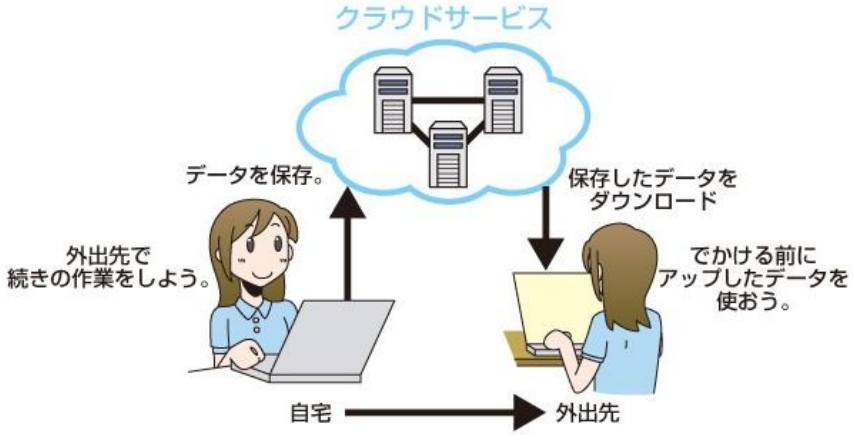


クラウドサービスとは

　クラウドサービスは、従来は手元のコンピュータで利用していたデータやソフトウェアを、ネットワーク経由で、利用できるサービスのことです。

　利用者側は、インターネットを介して、どの端末からでも、さまざまなサービスを利用することができます。

　このクラウドサービスを利用することで、機材の購入やシステムの構築、管理などにかかるとされていたさまざまな手間や時間の削減をはじめ、業務の効率化やコストダウンを図れる場合があります。



クラウドサービスは、主に以下の3つに分類されています。

◆ **SaaS（サース、サーズ：Software as a Service）**
　インターネット経由での、電子メール、グループウェア、顧客管理、財務会計などのソフトウェア機能の提供を行うサービス。

◆ **PaaS（パース：Platform as a Service）**
　インターネット経由での、仮想化されたアプリケーションサーバやデータベースなどアプリケーション実行用のプラットフォーム機能の提供を行うサービス。

◆ **IaaS（アイアース、イアース：Infrastructure as a Service）**
　インターネット経由で、デスクトップ仮想化や共有ディスクなど、ハードウェアやインフラ機能の提供を行うサービス。HaaS（Hardware as a Service）と呼ばれることもあります。

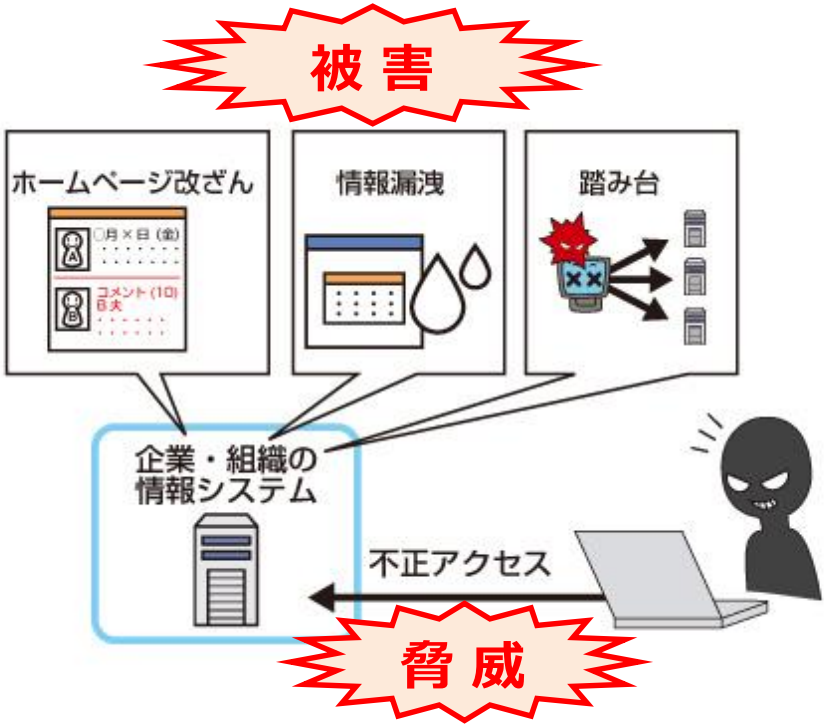
日本赤十字社
Japanese Red Cross Society

基礎知識２　ネット犯罪の脅威

インターネットを活用した脅威（外部攻撃）

　インターネットは世界中とつながっているため、インターネットにつながっている企業や組織のパソコンやシステムに不正で侵入される可能性は世界中のどこからでも考えられます。

　その結果、サーバや情報システムが停止してしまったり、重要情報が漏洩してしまったりと、企業や組織の業務やブランド・イメージなどに大きな影響を及ぼします。



被害者が加害者になりえる脅威

ウイルス感染したパソコンを踏み台にして、内部情報やシステムを攻撃したり、他のパソコンへ次々と攻撃繰り返すウイルスがあります。

感染させたパソコンを踏み台にして次のような攻撃をします。

- ◆迷惑メールの配信
- ◆インターネット上のサーバへの攻撃
- ◆ウイルスを増やすための感染活動
- ◆犯罪者との取引　等

ウイルスに感染したパソコンの所有者は被害者ではありますが、そのパソコンから大量に迷惑メールを送信したり別のサイトを攻撃したりするため、その被害を受けた人から見るとウイルスに操られたパソコンの所有者が加害者として判断される場合があります。

補足　ホームページの改ざんによって、企業のホームページを閲覧した人たちを悪意のあるWebサイトへ誘導したり、ウイルスに感染させようとする手口もあるので注意！

意図的ではない脅威（ヒューマンエラー）

インターネットの脅威は、外部からの攻撃だけではありません。
人による意図的ではない行為やシステムの障害などの事故も大きな情報セキュリティ上の脅威です。

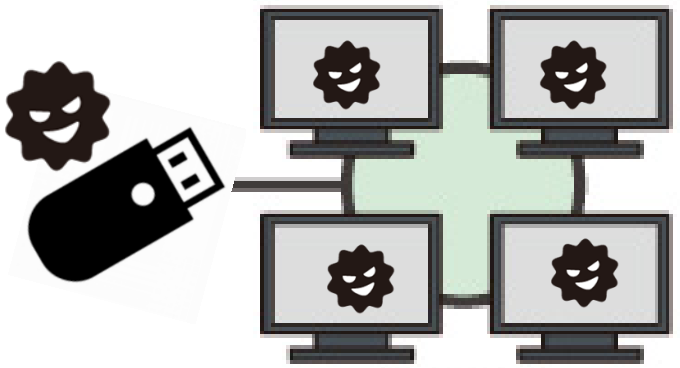
人は意図的ではなく、操作ミスや設定ミス、紛失など、いわゆる「つい、うっかり」の過失（ヒューマンエラー）にも脅威はあります。
電子メールの送り先を間違えたり、書類や記憶媒体の廃棄の方法を誤ったり、携帯電話やパソコンを紛失するといった過失が発生することで、顧客情報や機密情報が第三者へ漏洩することがあります。企業や組織における情報漏洩の原因の多くは、このような人の「つい、うっかり」やＩＴの使いこなし能力（ＩＴリテラシー）の不足によるものとされています。

組織内部の脅威・閉域網ネットワーク内にある脅威

組織内の内部犯行も想定される脅威の一つです。例えば、ウイルス感染したＵＳＢメモリを使用することで、社内の閉域網ネットワークにあるシステムがウイルス感染することも考えられます。

ウイルス感染する入口はインターネットだけではなく、インターネットが繋がっていないところからでもウイルス感染する可能性があることを考慮し、セキュリティ対策を考える必要があります。

例：私物のＵＳＢメモリは使わない
　　ＵＳＢメモリを使う前にウイルスチェックをしてから使用する等



閉域網ネットワーク

日本赤十字社
Japanese Red Cross Society

基礎知識３　ＩＴ資産の安全な運用

日本赤十字社
Japanese Red Cross Society

IDとパスワード

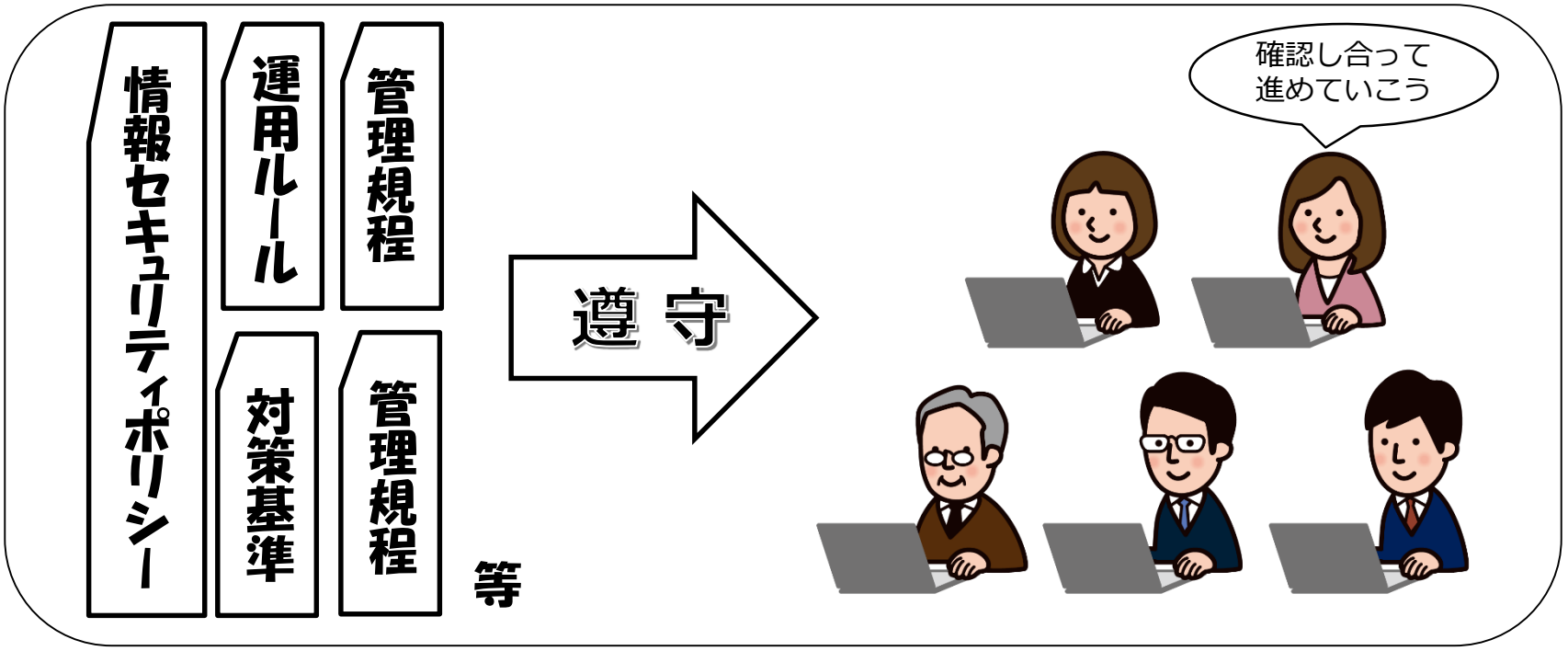
　IDとパスワードは、パソコンなどの情報機器やWeb上のサービスを利用する際に、許可された者であるかを識別し、本人を確認するための重要な情報です。

　適切なパスワードの設定と管理が大切です。また、定期的なパスワードもリスク回避の上で、重要となります。

事故・障害への備え

事故や障害が完全に発生しないようにすることは困難です。しかし、その発生確率を下げたり、被害を最小限に抑えることは可能です。

過失による事故を未然に防ぐために、組織での情報セキュリティポリシーを遵守し利用や運用のルールを守ることはもちろん、人の過失に備えて、例えば二重の確認チェックなどを行うなど、こうした事故への対策をしましょう。



事故・障害への備え

コンピュータ障害や自然災害等によって情報やデータファイルが失われることを想定して日常的に重要情報のバックアップを取ることや、利用するシステムには盗難や紛失への備えを行っているような信頼性の高い機能が備えておくことが必要です。

クラウドサービスのような外部業者のサービスを使っていた場合は、その業者側での障害で影響を受けることもあるため、事故や障害時の対応・対策を確認しておく必要があります。

（業務委託契約書の内容の確認等）

コンピュータ障害

等

自然災害

等

日本赤十字社の情報セキュリティ

日本赤十字社の情報セキュリティ体系

日本赤十字社情報セキュリティポリシー

日本赤十字社 情報セキュリティ基本方針	日本赤十字社における情報セキュリティ対策に関する基本的な考え方を示したもの
日本赤十字社 情報セキュリティ基本規程	日本赤十字社における情報セキュリティ対策の目的、対象、管理体制及び管理者の義務等を規程したもの
日本赤十字社 情報セキュリティ対策基準	施設単位で整備される、情報セキュリティ対策として実施すべき具体的な手順（ルール）を定めたもの
日本赤十字社 情報セキュリティ緊急時対応計画	施設 にて情報セキュリティ事故が発生した場合における対応手順、及び警察機関・関係省庁を含んだ連絡体制、応急措置等を定めたもの
各部門システム情報セキュリティ実施手順書	情報セキュリティ対策基準に基づき、各部門システムの詳細な情報セキュリティ対策の手順を定めたのも。

日本赤十字社の情報セキュリティ関連通知等

通知等	文書番号等	内容
「日本赤十字社情報セキュリティ基本方針」について	平成22年12月17日付 統情第20号社長通知	「情報資産のセキュリティ対策に万全を期す」日本赤十字社の情報セキュリティに対する基本姿勢、行動指針を示した
「日本赤十字社情報セキュリティ基本規程」の制定	平成22年12月17日付 本達丙第22号	日本赤十字社が遵守すべき情報セキュリティの基本事項を規定
個人情報を含む重要情報の適正管理について	平成27年6月9日 統情第31号	ー
支部・施設における情報セキュリティ対策基準の策定について	平成27年9月1日付 統情第44号	情報資産の性質や重要度に応じて講じなければならないセキュリティ対策の基準を定める（支部・施設単位で策定）
日本赤十字社情報セキュリティ緊急時対応計画の策定について	平成27年9月24日付 統情第53号	情報セキュリティインシデント発生時の本社・支部・施設の連絡体制や対応手順を定めたもの

日本赤十字社情報セキュリティ基本方針（一部抜粋）

目的

第１条 この規程は、日本赤十字社の保有する情報資産を保護・管理するために遵守すべき事項を定め、当該情報資産の機密を守り、故意や偶然という区分に関係なく、誤った使用や漏えい、改ざん、破壊等を防ぎ、情報を必要な時に確実に利用できるようにすることを目的とする。

適用範囲

第４条 この規程は、日本赤十字社の役員・職員、再雇用職員、嘱託職員、臨時職員、パートタイマー、日々雇い入れた者、その他日本赤十字社の情報資産を利用する者（以下「職員等」という。）に適用する。

職員等の責務

第５条 職員等は情報セキュリティの重要性について共通の認識を持ち、業務の遂行にあたり情報セキュリティポリシー並びに本社、支部及び施設で定める情報セキュリティ対策基準及び、実施手順を遵守しなければならない。

日本赤十字社情報セキュリティ緊急時対応計画（一部抜粋）

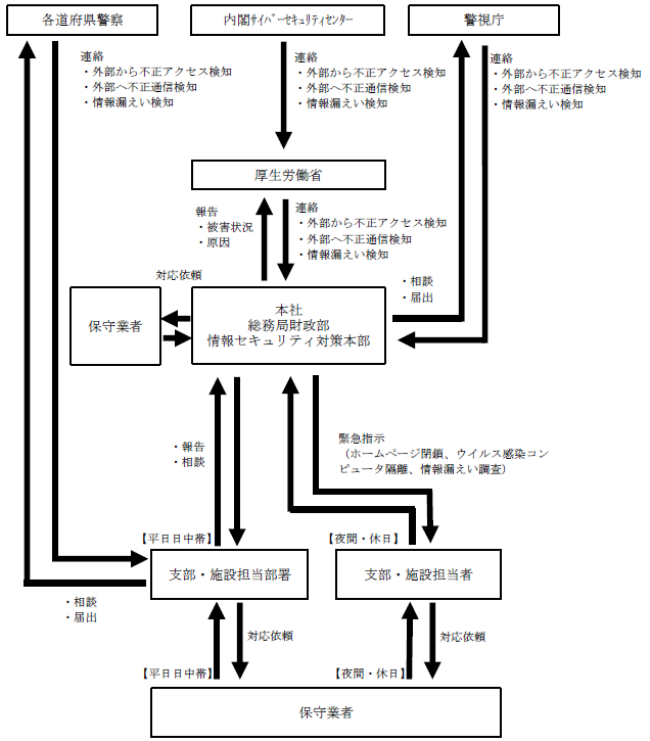
目的

本計画書は、日本赤十字社における 情報資産に対する事故、災害、情報セキュリティポリシー違反等による侵害が発生した場合、又は発生する恐れのある場合に備え、緊急時連絡体制、証拠保全、被害拡大の阻止、情報資産の復旧、再発防止等を計画し、その対応について定めることを目的とする。

緊急時連絡体制

緊急時の初動体制を円滑に行うため、 全社・本社・支部・施設・ 情報システム の単位で緊急時連絡体制を整備する。 また、報告事項は以下のとおりとし、別紙５「障害・事故等の発生及び再発防止等に関する報告書 」を総括情報セキュリティ管理者に提出する。

（１）対象となる情報資産
（２）障害区分
（３）概要（時間、場所、内容等）
（４）発生状況と被害の拡大予測
（５）発生原因
（６）その他留意事項



日本赤十字社緊急時全体体制図

情報セキュリティ対策本部の連絡先について

情報セキュリティ対策本部の連絡先

電話番号　　（03）3437-7593
メールアドレス　　infosec@jrc.or.jp