# 情報漏えいを防ぐための
# モバイルデバイス等
# 設定マニュアル

## ～安心・安全のための暗号利用法～

## ★★★　解説編　★★★


IPA 独立行政法人情報処理推進機構
セキュリティセンター

# 目次

# 1. はじめに

## 1.1　本書の内容及び位置付け

情報漏えい対策として「社外に秘密情報を持ち運ぶな」とのルールを決めていても、現実には自宅や外出先などで業務を行うために必要な秘密情報を外部に持ち運ぶ例は後を絶ちません。

もちろん、従業員のモラルだけに依存するのではなく、システム的に社外への秘密情報の持ち運びができないようにすることも可能であり、実際にそのための対策システムやツールも販売されています。しかし、そういったシステムやツールを導入するには多額の費用がかかるうえに、現場の実情を無視した一律の規制は業務効率の著しい低下を招く恐れがあります。

また現実問題として、在宅勤務の奨励やスマートフォン・タブレットのビジネス利用の拡大など、従来にも増して秘密情報を社外に持ち運んで業務を行う機会が増えています。こういったケースでは、社外でも自由に秘密情報が利用できる利便性によって業務効率の改善につながることも多く、「社外に秘密情報を持ち運ぶな」といったルールそのものを見直す必要に迫られるケースもあるでしょう。

しかし一方で、「社外に秘密情報を持ち運ぶことを許可」することは、確実に秘密情報の漏えいリスクを高めることになります。そこで、少しでも情報漏えいリスクを低減するために、情報の持ち運びに関するセキュリティ対策や在宅勤務におけるセキュリティ対策、スマートフォン・タブレット・ノートパソコンの業務利用に関するセキュリティ対策などの各種ガイドラインも多数公開されています。

多くのガイドラインでは、多数の考慮すべき対策が網羅的に列挙されており、そのなかのひとつに「(情報を持ち運ぶ際に) 暗号化をする」ことが含まれています。

**端末を紛失したなどの万が一の際、情報漏えいを防ぐ最後の砦となるのは「情報が暗号化されていたかどうか」**です。しかし、どのガイドラインでも、具体的な暗号化の手法まで記載されていることはほとんどありません。

本マニュアルでは、**「情報を持ち運ぶ際に暗号化をする」という行為として、具体的に「何をすれば何が守られ、何が守れないのか」に特化して解説**するものです。セキュリティ対策上の各種ガイドラインや社内のセキュリティルールをベースとして、**暗号化のハウツー集**として用いることを想定しています。本マニュアルが、外部への安全な情報持ち運びのための適切な暗号利用を進める一助となれば幸いです。

## 1.2　本書が対象とする読者

本マニュアルは、セキュリティ対策実施の責任者や担当者だけでなく、企業・組織の全従業員を対象としています。また、個人の私的利用においても有効であると考えています。

## 1.3　本書が対象とする範囲

情報漏えいでは「不正アクセス」や「内部犯行」、「不正持ち出し」による事件が大きく報道されます。

しかし、NPO日本ネットワークセキュリティ協会（JNSA）の「JNSA 2011 年情報セキュリティインシデントに関する調査報告書」[1]によれば、2011 年に発生したインシデント件数 1,551 件のうち、実際の情報漏えいの原因としては「誤操作（34.8%）」「管理ミス（32.0%）」「紛失・置忘れ（13.7%）」「盗難（6.6%）」が上位であり、これらの合計だけで 90%弱を占めています（図 1）。

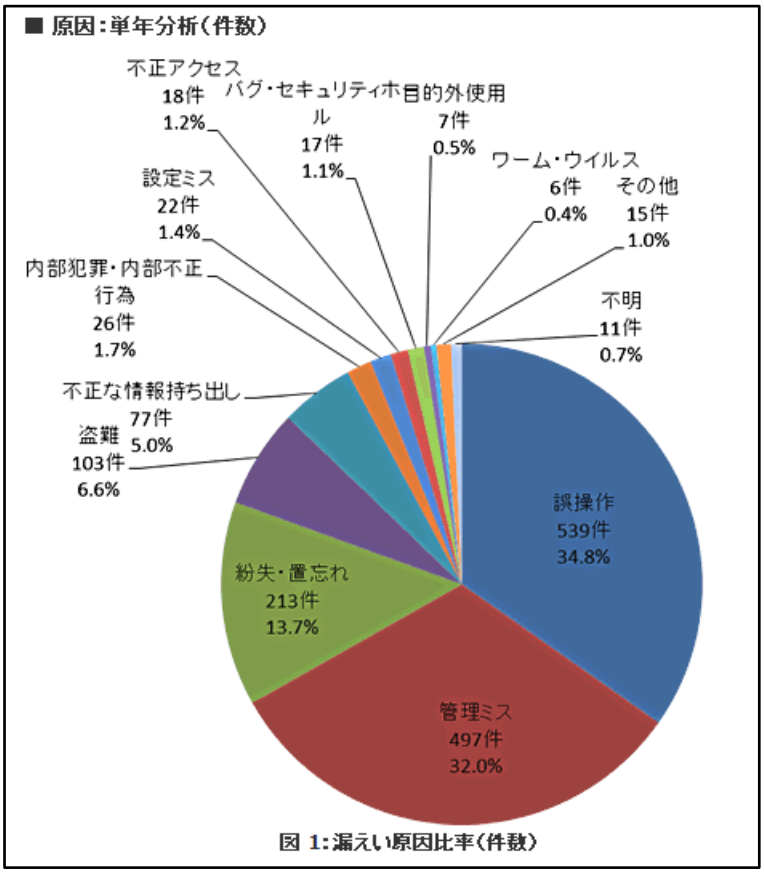



**図 1　漏えい原因比率（件数）[2]**

また、「JNSA 2011 年情報セキュリティインシデントに関する調査報告書 ～発生確率編～」によれば、実際に携帯電話・パソコン・USB メモリなどの紛失や盗難を経験したことがある割合は 2%前後もあり、このアンケート調査結果だけで公表されているインシデント件数を上回っています（図 2）。このことは、紛失・盗難として表面化したインシデント件数が氷山の一角である可能性を示しています。

---

[1] http://www.jnsa.org/result/incident/2011.html

[2] NPO 日本ネットワークセキュリティ協会「2011 年情報セキュリティインシデントに関する調査報告書」より引用。http://www.jnsa.org/result/incident/2011.html

つまり、一般の従業員にとっては、日常業務遂行のなかに潜む意図せざる情報漏えいを防ぐことのほうがむしろ重要であるとさえ言えます。

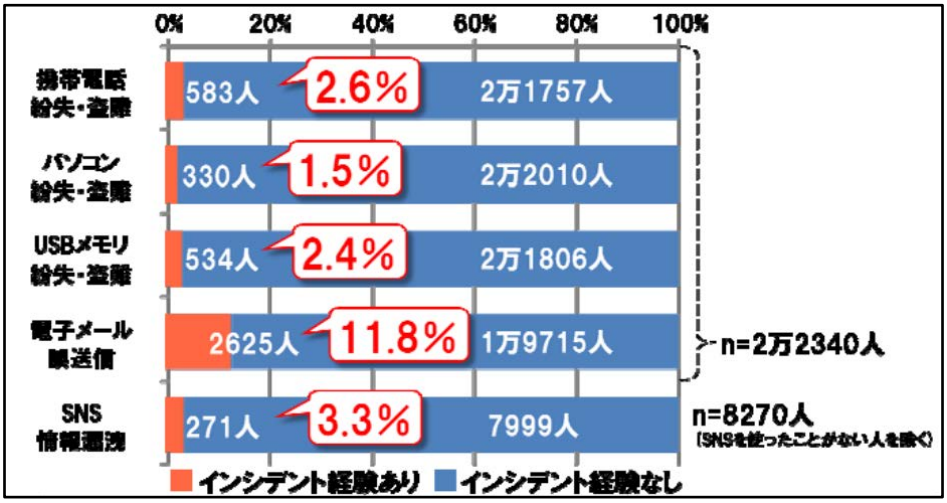



図 2　漏えい原因比率（件数）[3]

本マニュアルでは、企業・組織内あるいは私的利用で、個人情報や企業情報などの秘密情報をノートパソコンやスマートフォン、USB メモリ等の可搬媒体を活用して外部に持ち運ぶことを想定し、こういった**可搬媒体で情報を持ち運ぶ際に、紛失や盗難等をはじめとした意図せざる情報漏えいに対する対策として、どのような情報をどのように暗号化しておくべきか**、について述べています。

これによって、万が一、紛失や盗難をした場合であっても、その可搬媒体の拾得者が権限なく暗号化を解除する（「解読する」といいます）ことを防止し、外部に秘密情報が漏えいするリスクを大幅に低減することができます。なお、秘密情報を利用する権限がない利用者が意図的かつ悪意を持って不正に可搬媒体に秘密情報を入れて持ち出したとしても、その秘密情報が適切に暗号化されていれば、外部に秘密情報が漏えいするリスクも低減できます。

一方で、従業員が**自ら利用する権限のある秘密情報を意図的かつ悪意を持って不正に持ち出すケースに対する対策は今回の本マニュアルの対象外**とします。これは、秘密情報を利用する権限を有する利用者には暗号化を解除する（「復号する」といいます）権限が付与されていますので、たとえ秘密情報が暗号化されて持ち出されたとしても、外部で元の秘密情報に復号して漏えいさせることが可能です。

つまり、**秘密情報を利用する権限を有する利用者が意図的かつ悪意をもって不正に持ち出す際には、暗号化だけの対策では守りきれない**ことに注意してください。

[3] NPO 日本ネットワークセキュリティ協会「2011 年情報セキュリティインシデントに関する調査報告書 ～発生確率編～」より引用。http://www.jnsa.org/result/incident/2011_probability.html

# 2. 情報漏えい対策が正しく機能するために知っておくべきこと

情報漏えいを防ぐ最後の砦となるのは「情報が暗号化されていたかどうか」ですが、暗号の話となると、途端に難しい、よくわからない、といって敬遠されがちです。

そこで、本マニュアルでは、あえて**暗号アルゴリズムの技術的な中身は説明しません**。

その代わり、暗号製品が情報漏えい対策として正しく安全に機能するために**最低限知っておいてほしいことだけを説明**します。「暗号アルゴリズムがどのように動作するか」を知る必要はありませんが、**「暗号製品を使って情報漏えい対策が正しく安全に機能するためには、何に注意しなければいけないのか」を理解**してください。

## 2.1　端末ロックを設定するだけでは不十分　～ 暗号化の必要性 ～

ノートパソコンやスマートフォンなどの端末には、「暗号化」とは別に「端末ロック（画面ロック、アカウント認証、ログイン認証などと表示されることもあります）」というセキュリティ機能があります。これは、端末を利用しないときにはロック状態にして端末の入出力操作を受け付けないようにしておき、利用時に正規の利用者であるかどうかを確認したうえで端末のロックを解除して入出力操作ができるようにする機能です（図 3）。

どの端末にも標準で搭載されており、設定をオンにするだけで利用可能になります。

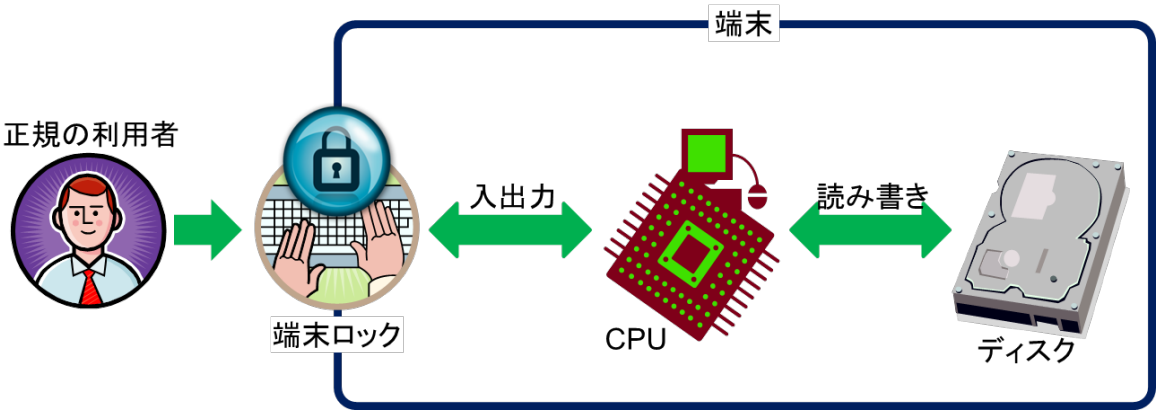



図 3　正規の利用者と端末ロックの関係

ただし、「端末ロック」の文字通り、**端末での入出力操作をロックしているにすぎません**ので、設定をオンにしたからと言って**端末内の情報が自動的に暗号化されるわけではありません**。

つまり、別の手段で端末内の情報が暗号化されていない限り、何らかの手段で端末ロック機能を回避することができれば、データを読み出して情報を見ることができることになります。例えば、端末ロックを回避する比較的簡単な手段としては、①管理者権限をもつ利用者名によるログイン（管理者になりすますなど）、②ロックされている端末 A のハードディスクをロックされていない別端末 B に取り付ける、などの方法があります（図 4）。

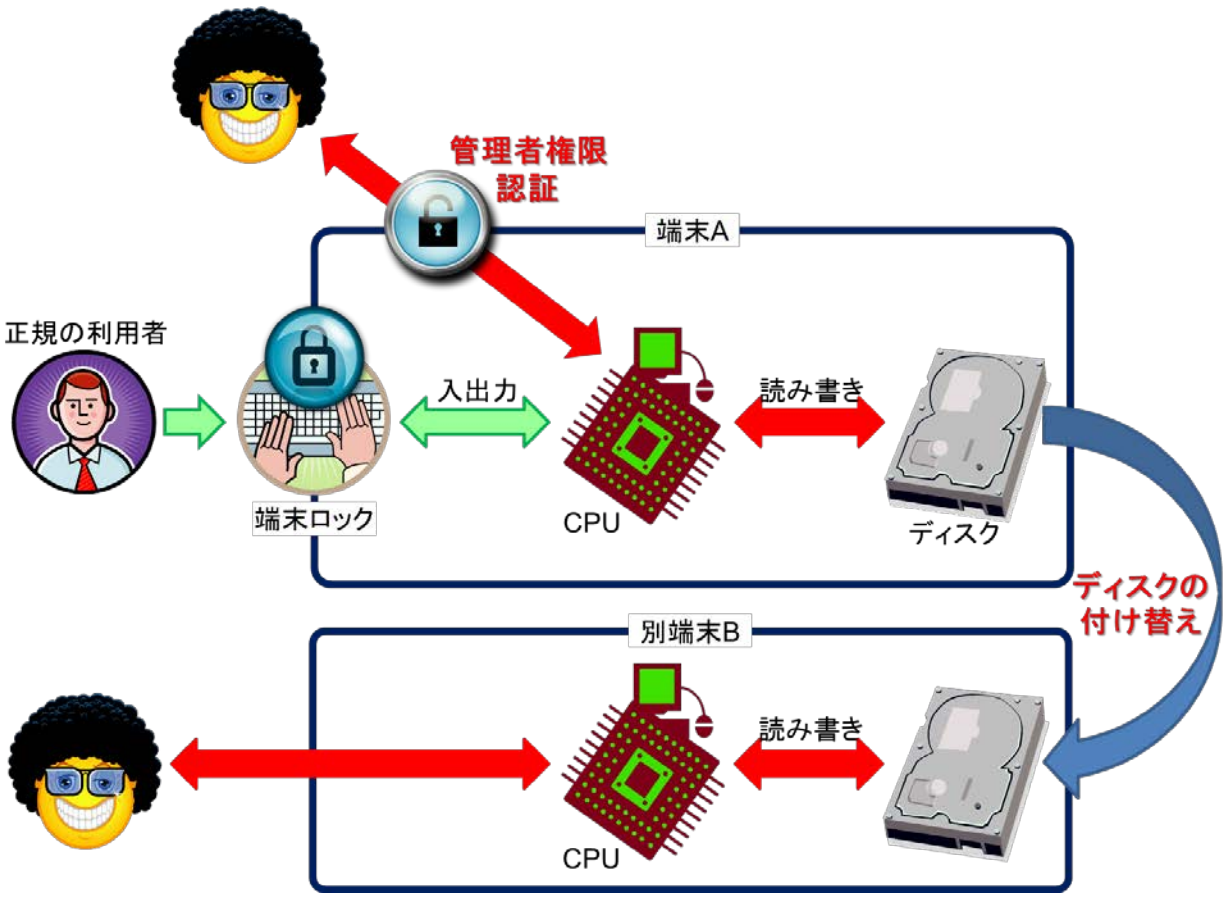



図 4　端末ロックの回避例

## 2.2　暗号化の仕組み

情報の暗号化とは、共通のデータ変換手順として決められた**「暗号アルゴリズム」**にしたがって、他者と区別するための制御情報である**「暗号鍵」**を用いて、暗号化したい情報（「平文」といいます）を、第三者が中身を読むことができないランダム化された情報（「暗号文」といいます）に変換したり、逆に暗号文を元の平文に戻したりするための処理です。

ここで知っておいてほしい点は、**暗号化処理のためには「暗号アルゴリズム」だけでなく、「暗号鍵」も使う必要がある**ということです。

しかし、実際に情報の暗号化をする際、利用者が「暗号アルゴリズムはどうするか？」「暗号鍵はどうしようか？」などと悩むことはほとんどありません。

それは、暗号アルゴリズムや暗号鍵を利用者が直接的に制御することはなく、すべては OS やアプリケーション、暗号製品などのシステムの制御下で動作しているからです。つまり、**システムが正規の利用者であると確認（利用者認証、ユーザ認証）**したうえで、**その利用者の代行として情報の暗号化処理を統制**していることになります（図 5）。

通常、暗号鍵は安全な形で保存されており、平文を見る権限がある利用者だけがその暗号鍵を利用することができるようにシステムが制御しています。

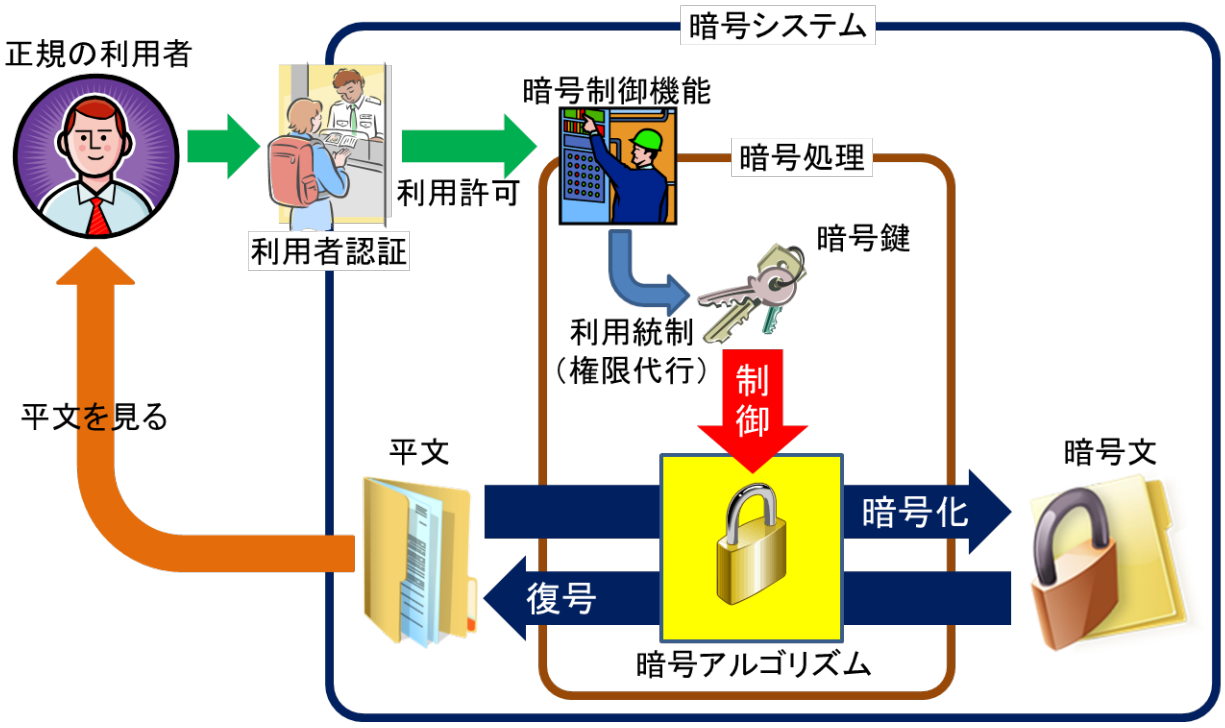



図 5　正規の利用者と暗号化処理の関係

## 【コラム①】暗号アルゴリズム ～共通鍵暗号と公開鍵暗号～

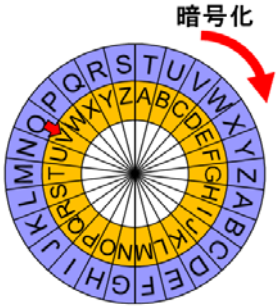
仮に膨大な量（例えば、約 340 万×1 京×1 京個以上）の平文と暗号文の対応表をいくつも持つことができるならば暗号アルゴリズムは必要ありません。しかし、現実にはそれだけの量の対応表を持つことは不可能です。

そこで、対応表を持つ代わりに、平文と暗号文とをどのように対応させるかを決める共通のデータ変換手順を作り、その手順に従って平文と暗号文の対応を求める方法ができました。それが「暗号アルゴリズム」です。具体的なデータ変換手順としては、ある文字を別の文字に置き換える方法（換字といいます）、複数の文字の位置を入れ替える方法（転置やアナグラムといいます）、四則演算を駆使する方法など、様々な方法があり、それらが複雑に組み合わさって暗号アルゴリズムとしての手順が作られます。

例えば、古代ローマ時代に作られたシーザー暗号は、「暗号アルゴリズム」と「暗号鍵」の関係が非常にわかりやすい例といえます。

シーザー暗号の暗号アルゴリズムは「X 文字分だけ先にずらす（＝X 個先の文字に置き換える）」です。この X の値を変えると暗号文が変わるため、X が「暗号鍵」になります。

例えば「OPEN」を暗号化する場合、X=1 なら「OPEN」→「PQFO」に、X=7 なら「OPEN」→「VWLU」となります。




なお、復号のためのアルゴリズムは「X 文字後ろに戻す」であり、暗号鍵は同じ X の値を使います。

シーザー暗号と同じように、暗号化処理と復号処理で共通の暗号鍵を使うものを「共通鍵暗号」といい、古代ローマ時代から延々と使われてきた手法です。もちろん、時代とともに暗号アルゴリズム自体は非常に複雑かつ精緻なものになってきていますが、共通の暗号鍵を使うという点についてはまったく変わっていません。

一方、1970 年代に暗号化処理と復号処理で使う暗号鍵が異なるタイプの暗号方式が発明されました。もちろん、ある特定の関係にある 2 つの鍵ですが、復号処理で使う暗号鍵だけを秘密にしておけば暗号アルゴリズムとしての安全性が保たれ、暗号化処理で使う暗号鍵は公開してもよいという特長から、「公開鍵暗号」と呼ばれるようになりました。

## 2.3　暗号化しさえすればそれだけで安心？ ～使い方を間違えると情報漏えい対策として安全に機能しない～

暗号化された情報（暗号文）の内容（平文）を見るためには、暗号文を元の平文に戻すために必要な「暗号鍵」を使う必要があります。

**平文を見る権限がある利用者（有権限者）に対しては、システムがその暗号鍵を自由に利用できるように制御**しますので、有権限者は何ら問題なく暗号文を平文に戻すことができます。このことを「復号」と呼びます。

ところで、「暗号化された情報の内容（平文）を見ることができたので、その暗号の解読ができた」といった記事を目にすることがあります。確かに、暗号アルゴリズムを解読することができれば平文を見ることができます。

しかし、「暗号化された情報の内容（平文）を見る」ことと「暗号アルゴリズムが解読できる」ことは必ずしもイコールではありません。**何らかの不正な手段で「暗号鍵」を使うことができるようになれば、たとえ平文を見る権限がない利用者（無権限者）であっても平文を見ることができる**からです。

そのような不正な手段としては大きく 3 つのケースが考えられます（図 6）。このうちのどれか一つでも不正に利用されると、無権限者であっても平文を見ることができる恐れが高まります。

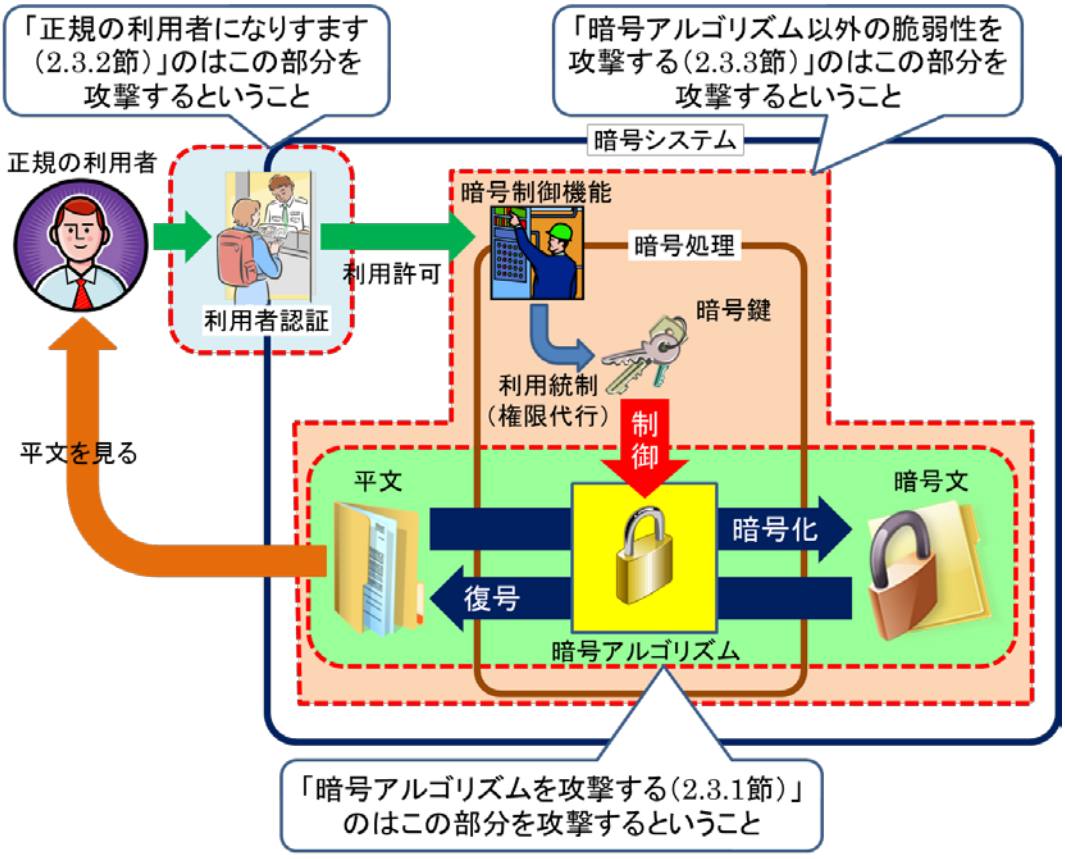



図 6　不正な手段として攻撃者に狙われる場所

### 2.3.1　暗号アルゴリズム自体の脆弱性が悪用されるケース

いわゆる「暗号解読」というもので、暗号アルゴリズム自体がもつわずかな脆弱性を巧みに利用して、強引に暗号鍵を求めるやり方です。暗号鍵そのものが分かれば、システムの制御下から外れて、独自に暗号文から平文を求めることも可能になります。

このケースに対しては、**強固な暗号アルゴリズムを使って、暗号解読自体を困難にする以外の対策はありません**。その際、“自称”強固な暗号アルゴリズムではいけません。どのような暗号アルゴリズムが強固な暗号アルゴリズムと判断されるのかは、2.4.1 節を参照してください。

### 2.3.2　正規の利用者になりすまされるケース

たとえ正規の利用者でなくても、「正規の利用者である」とシステムに誤認させることさえできれば、その人に対して正規の利用者と同様の権限が自動的に付与され、システムの制御下で暗号鍵を自由に使うことができるようになります。結果として、暗号化された情報の内容（平文）を無制限に見ることができるようになります。

典型的な例として、フィッシングサイト [4]に誘導してID／パスワードを盗み出す行為は、攻撃者が正規の利用者になりすますための情報を入手しようとしていることに他なりません。

このケースでは、**暗号アルゴリズムが強固であるかどうかは関係がない**ことに注意してください。**多くの場合、暗号アルゴリズムそのものの解読よりもはるかに容易な攻撃方法**となります。詳しくは、2.4.2 節を参照してください。

### 2.3.3　暗号アルゴリズム以外の脆弱性が利用されるケース

「強固な暗号アルゴリズムを使っていたはずなのに、正規の利用者になりすますことなく、暗号文が実際に解読され、暗号化された情報の内容（平文）を見ることができた」といった事象がたまに発生することがあります。

この場合に考えられる原因としては 2 つあります。

一つは、**ある特定の暗号製品に搭載された暗号アルゴリズムの実装もしくは暗号鍵の運用管理などに脆弱性**があった場合です。この脆弱性を利用して、システムそのものが乗っ取られたり、暗号鍵が不正に入手される可能性があります。

暗号アルゴリズムの実装の脆弱性を利用した攻撃方法は「実装攻撃」と一般に呼ばれ、暗号製品に対する直接的な攻撃方法です。この攻撃方法では、暗号化処理の入出力データの値（平文や暗号文）だけでなく、暗号化プロセス実行中の内部データや消費電力・処理時間の変動を計測するなどして、暗号化処理中のデータや暗号鍵に依存する情報を入手し、それらの情報を解析して暗号鍵を直接推定

[4] ID／パスワード、クレジットカード番号などの情報を盗むために、本物のウェブサイトに似せて作った偽物のウェブサイトのこと

します。

暗号鍵の運用管理の脆弱性としては、例えば、本来秘密にされているはずの暗号鍵の“保存場所”を直接探し当てられ、そこに書かれているデータ値から暗号鍵を割り出す、といったケースがあります。身近な具体例としては、DVDプレーヤーに搭載されたコピーガード機能（CSS[5]）で利用する暗号鍵やデジタル放送における著作権管理に使われているB-CASカードに搭載された暗号鍵が見つけられたケースなどがあります。

もう一つは、暗号アルゴリズムを使ったプロトコルなどの上位の仕組みのなかで、**暗号化を行うためのデータの扱い方に脆弱性**があった場合です。

プロトコルなどの上位の仕組みがデータを扱う際には、例えば、ヘッダー情報と呼ばれる特定の情報や､データの長さを整えるなどのためにパディングと呼ばれる情報が多く付加されます｡これらは、一般に仕様として使い方が定められているので、攻撃者がその仕組みを容易に知ることができる情報となります。

そのため、この部分に脆弱性があると、付加される情報を攻撃者がうまく利用して、調べるべき暗号鍵の候補を大きく限定できたり、メッセージを一つ一つ暗号化して攻撃目標とした暗号文と一致するかを実際に確認できるようになることがあります。例えば、暗号文のどの部分に入札金額に相当する情報があり、またそれ以外の部分にどのような情報が付加されているかを攻撃者が知っているならば、入札金額が書かれている個所に様々な金額を入れて暗号化し、その結果が攻撃対象とした暗号文と一致すればその金額が入札金額だとわかります。ここでのポイントは、元の情報（入札金額）を知るためには、たくさんのメッセージの中から探す必要はなく、ある範囲の金額の中から探せばよい、ということです。

このように、結果として、強固な暗号アルゴリズムを使っていても、暗号鍵が特定できたり、メッセージと暗号文の対応表から元の情報(平文)を見つけ出すといったことができる可能性があります。

なお､この種の攻撃の多くは中間者攻撃 (Man-in-the-middle 攻撃) と呼ばれる手法が使われます。この手法では､攻撃のターゲットにされた利用者とその利用者の通信相手との間に攻撃者が“能動的”に入り込んで、通信データに細工できることが条件となります。そのため、両者の通信路中に物理的に入り込むケースのほか、利用者の端末にウイルス感染させて通信相手自体を攻撃者に設定させることで必要な情報を攻撃者が得るケースが想定されます。

もちろん、暗号製品やシステムを製造する段階では、できる限り、こういった脆弱性が入らないように配慮していると考えられます。しかし、対策には様々なコストがかかりますので、製造コストや販売価格の観点から見て、こういった種類の脆弱性が発生すること自体を完全に取り除くことは極めて困難です。また、ソフトウェアの実装バグを完全になくすことも現実には不可能です。

[5] Content Scramble System。現在の DVD/Blu-ray プレーヤーには、CSS より高機能な AACS (Advanced Access Content System)が搭載されている

もっとも、**暗号アルゴリズム自体が解読されたわけではありません**ので、発見された脆弱性に対して実装上の修正を施したり、運用でうまく回避したりすることによって、暗号化された情報の内容（平文）が見られることを防ぐことができます。その意味で、もっとも脅威となる可能性が高いのは、**攻撃者がそういった脆弱性を使って攻撃できるようになったときから、その脆弱性を修正する対策パッチが適用されるまでの期間**となります。

このほかに注意することとして、基本的に暗号化処理の動作は不可視であることから、**暗号製品の信頼性は、事実上、製造会社・販売会社に全面的に依存**しているという暗号製品特有の問題があります。そこで、暗号製品として安全に利用できることを中立的かつ第三者的に確認・検証し、安全性が確認されたものに対してお墨付きを与える「セキュリティ認証制度」が作られています。詳しくは、2.4.3.2 節を参照してください。

## 【コラム②】実装攻撃ってなに？

最近の強固な暗号アルゴリズムでは仕様上の脆弱性が少なくなり、現実的に暗号解読される危険性はほとんど無視できる状況になりました。そこで、暗号アルゴリズムそのものの脆弱性を利用した攻撃手法ではなく、実装した暗号製品に対する直接的な攻撃方法である「実装攻撃」に対する研究が幅広く行われるようになってきています。

実装攻撃では、以下の 5 つの手法がよく知られており、そのうちプローブ攻撃は侵入型攻撃、それ以外を非侵入型攻撃と呼ぶ場合もあります。

- チップ内の信号線などを直接タッピングして、暗号化処理中のデータや暗号鍵などを直接読み取る「プローブ攻撃」
- 暗号化処理中の消費電力の変動を計測・解析して暗号鍵を割り出す「電力解析攻撃」
- 暗号化処理にかかる時間差を計測・解析して暗号鍵を割り出す「タイミング攻撃」
- 故意に処理エラーを発生させて正しい処理結果との差分を観測・解析して暗号鍵を割り出す「故障利用攻撃」
- 暗号製品が出す電磁波を観測・解析して暗号化処理中のデータや暗号鍵など読み取る「電磁波解析攻撃（テンペスト攻撃)」

暗号製品の実装によっては、暗号化処理をするときに使っている暗号鍵の値に依存して消費電力や処理時間などが微妙に変動することを、オシロスコープなどの比較的簡単・安価な計測機器を使って観測できることがあります。また、電磁波は大なり小なり必ず外部に放射されているため、アンテナなどで傍受できることがあります。

この種の情報は、大掛かりな測定装置を必要とせず、外部から比較的計測がしやすいため、これらの情報を計測・解析して暗号鍵を割り出す電力解析攻撃やタイミング攻撃、電磁波解析攻撃などのことを特にサイドチャネル攻撃といい、現在、主流となっている実装攻撃手法です。

例えば、もっとも簡単な電力解析攻撃の例としては、暗号鍵の値が「0」であれば処理をしない、「1」であれば大きな値同士の掛け算をする、といった場合、もしあるタイミングでの消費電力がゼロに近く、別のタイミングでの消費電力が大きく跳ね上がるようなことがあれば、前者の暗号鍵の値は「0」、後者の値は「1」と判断していくものです（図 7）。

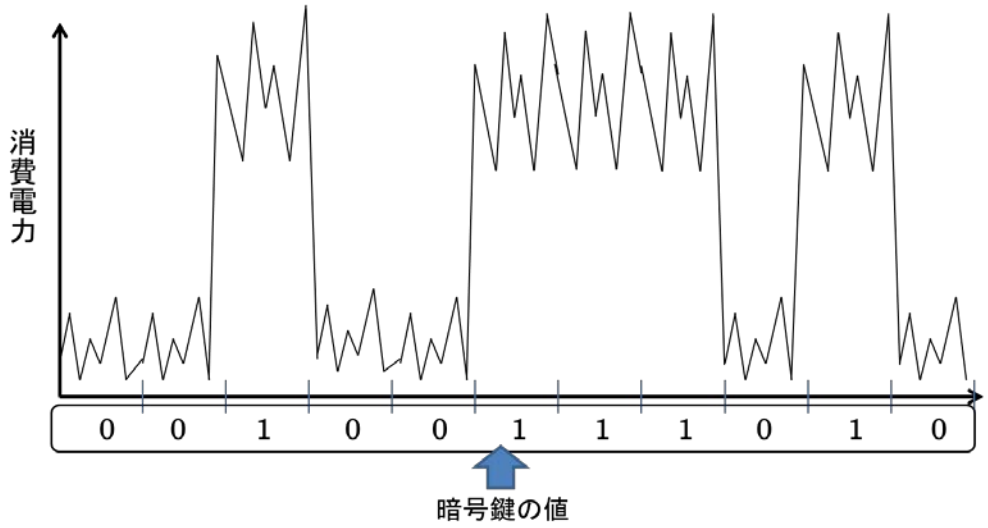



**図 7　消費電力の変化から暗号鍵がわかることもある**

対策としては、例えば、実際には処理をしない時間帯でもあえてジャミング処理（消費電力を上げるためだけに行う処理）を発生させることで、全体としてみると消費電力の変動が非常に小さくなるようにする、などがあります。

## 2.4　情報漏えい対策として正しく安全に機能するために必要なこと

### 2.4.1　第三者検証された安全な暗号アルゴリズムを使う ～電子政府推奨暗号とは～

暗号化するために使った暗号アルゴリズムが安全でなければ、情報を暗号化する意味がありません。しかし、たくさんある暗号アルゴリズムのなかから、どの暗号アルゴリズムが安全であるかを判断することは容易ではありません。なぜなら、どの暗号製品であっても、「使っている暗号アルゴリズムは安全」と謳っているからです。

そこで、本マニュアルとしては、総務省及び経済産業省が公表している**電子政府推奨暗号リスト**[6]**に掲載されている暗号アルゴリズム（表 1）を採用している暗号製品・システムを選択**することを推奨します。

電子政府推奨暗号リストとは、総務省及び経済産業省が共同で運営しているCRYPTRECプロジェクト[7]において、日本の暗号分野の有識者らが十分な安全性及び実装性能を持つと確認・検証した暗号アルゴリズムのうち、市場における利用実績が十分であるか、もしくは今後の普及が見込まれると判断されたものをまとめたリストであり、当該暗号アルゴリズムの利用を推奨するとされているものです。

各府省庁が情報システムを構築する際にも、内閣官房情報セキュリティセンターが公表している「政府機関の情報セキュリティ対策における政府機関統一管理基準及び政府機関統一技術基準」[8]に基づき、このリストに掲載された暗号アルゴリズムを使用することが遵守事項として定められています。

**表 1　電子政府推奨暗号リスト**

| 技術分類 | | 暗号アルゴリズム名 |
|---|---|---|
| 公開鍵暗号 | 署名 | DSA，ECDSA，RSA-PSS，RSASSA-PKCS1-v1_5 |
| | 守秘 | RSA-OAEP |
| | 鍵共有 | DH，ECDH |
| 共通鍵暗号 | 64 ビットブロック暗号 | 3-key Triple DES |
| | **128 ビットブロック暗号** | **AES，Camellia** |
| | **ストリーム暗号** | **KCipher-2** |
| ハッシュ関数 | | SHA-256，SHA-384，SHA-512 |
| 暗号利用モード | 秘匿モード | CBC，CFB，CTR，OFB |
| | 認証付き秘匿モード | CCM，GCM |
| メッセージ認証コード | | CMAC，HMAC |
| エンティティ認証 | | ISO/IEC 9798-2，ISO/IEC 9798-3 |

[6] http://search.e-gov.go.jp/servlet/PcmFileDownload?seqNo=0000097652
[7] Cryptography Research and Evaluation Committees の略であり、電子政府推奨暗号の安全性を評価・監視し、暗号技術の適切な実装法・運用法を調査・検討するプロジェクト
[8] http://www.nisc.go.jp/active/general/kijun01.html

まずは、暗号製品のパンフレットや取扱説明書などに、表 1 にある暗号アルゴリズム名のいずれかが記載されていることを確認し、それが記載されている暗号製品を選ぶようにしてください。とりわけ、情報の暗号化には共通鍵暗号が一般に利用されますので、**情報の暗号化の視点からは「AES、Camellia、KCipher-2」のうちのいずれかが明記**されているものが望ましいといえます。

ランダムに生成された暗号鍵であれば、これらの暗号アルゴリズムで暗号化された暗号文を解読するために必要となる計算量は $2^{128}$ 以上（約 340 万×1 京×1 京個以上）であり、**パスワードで同じ安全性を持たせようとすれば、英数字（0-9, A-Z, a-z）なら 22 文字以上もの長さが必要になる安全性**を持っています。

このことが意味するところは、暗号化された元の情報（平文）を見るにあたって、現在のところ一つ一つ暗号鍵を調べる全数探索で正しい暗号鍵を見つけ出す方法がもっとも効果的な暗号解読手法であるものの、実際に「全数探索で暗号解読する」ことは非現実的だということです。

暗号アルゴリズムにも寿命があるとか、どんな暗号アルゴリズムでもいつかは破られる、という話を耳にする機会があるかもしれませんが､少なくとも電子政府推奨暗号で暗号化された暗号文が 5 年、10 年といった単位で現実に暗号解読され、その内容（平文）が見られる可能性はほとんどゼロです。しかも、暗号化されていない情報なら即座に内容を見ることができることと比較すれば、暗号化しておくだけのことで劇的に情報漏えいリスクを低くできます。

## 【コラム③】「第三者検証された安全な暗号アルゴリズム」の重要性

安全性の観点において、暗号アルゴリズムを公開することのメリットは、逆説的ですが、世界第一線級の暗号研究者からできるだけ多くの暗号解読の挑戦を受けることにあります。しかも、暗号研究者が設定する暗号解読手法は、現実には到底ありえないような状況を想定したうえで、それでもなお暗号設計時の安全性を満たしているかどうか（あるいは許容できるレベルの安全性低下で済んでいるか）を厳しく評価するものです。

ここで想定する状況とは、例えば、「攻撃者は、自ら自由に選んだ膨大な量の暗号文に対応する内容（平文）をすべて教えてもらえる（選択暗号文攻撃と呼ばれる暗号解読手法)」とか、「世界中のコンピュータすべてを合わせた計算能力をはるかに超える計算能力を暗号解読に費やしてもよい（例えば 1 兆テラバイトの記憶容量と京コンピュータ 1 兆台分の計算能力を使う)」といったものも含まれます。

そして、それらの挑戦をことごとく跳ね返した暗号アルゴリズムだけが「安全性が高い」との評価を国際的に得ることができます。世界第一線級の暗号研究者が多数評価している以上、簡単に新たな暗号解読手法が見出されるとは考えにくいためです。

実際、今回電子政府推奨暗号リストに選定された暗号アルゴリズムはそういった関門をくぐり抜けてきたものばかりであり、少なくとも現時点で知られているような、あるいは近い将来見つ

かるかもしれない極めて強力な暗号解読手法に対しては、実用上の安全性を損なう事態になる可能性は極めて低いと判断されています。

一方、今までに無数の暗号アルゴリズムが作られながら、国際的に安全であるとの評価を得ている暗号アルゴリズムが少ないということは、言い換えると暗号研究者の挑戦に敗れ、生き残れなかった暗号アルゴリズムが数多くあるということになります。

また、「暗号アルゴリズムを秘匿すれば暗号解読にさらされることはない」というのが誤解であることは、過去に「秘匿だったはずの暗号アルゴリズム」が攻撃対象になった例があることからも明らかです。一番有名なところでは RC4 があり、リバースエンジニアリングによって RC4 のアルゴリズムの詳細が明らかにされました。

リバースエンジニアリングという行為が不法だという意見も出そうですが、暗号アルゴリズムを解読する行為自体が、研究目的を除けば、もともと不法行為となってもよいという動機のうえで行われています。暗号解読を目的とする以上、攻撃者はすべての攻撃手段を利用するのは当然であり、リバースエンジニアリングを問題視することはナンセンスといえます。

暗号アルゴリズムが秘匿されているから暗号解読されないのではなく、単に攻撃者の暗号解読の対象になっていないだけにすぎないと理解すべきです。

その意味で、秘匿された暗号アルゴリズムの最大の欠点は、暗号設計者以外の安全性検証を受けていないことに他なりません。

今までの暗号解読の歴史は、暗号設計者が思いもよらなかった脆弱性を突かれて暗号アルゴリズムが解読され、暗号文から元の平文に戻すことができるようになった歴史でもあります。

## 2.4.2　利用者を正しく見極める ～なりすまされないために注意すること～

### 2.4.2.1　正規の利用者かどうかを判断するための認証手段

システムが正規の利用者かどうかを判断（「利用者認証」「ユーザ認証」といいます）する認証手段は大きく分けると以下の 3 種類あり、これらが併用されることもあります。

いずれの認証手段も、正規の利用者**だけが**知っている・持っていることを前提としています。

- 「知識」を利用する認証手段：
  正規の利用者**“だけが知っている情報（知識）”**をその人が知っているか否かで判断する
- 「所持」を利用する認証手段：
  正規の利用者**“だけが持っているモノ（所持品）”**をその人が持っているか否かで判断する
- 「存在」を利用する認証手段：
  正規の利用者の**“身に備わっている特徴（利用者自身の存在）”**でその人か否かを判断する

**表 2　システムが正規の利用者かどうかを判断する認証手段**

| 認証手段の概要と具体例 | | 利点 | 欠点 |
|---|---|---|---|
| 「知識」を利用する手段 | ● パスワード<br>● パスフレーズ<br>● 暗証番号<br>● ピクチャーパスワード | ● 運用コストが安い<br>● 特別な装置が不要で、非常に簡便 | ● 複雑すぎる「知識」は記憶できない<br>● 簡単な「知識」であれば、正規の利用者でなくでも、「知識」を推定して正規の利用者になりすますことができる<br>● 「知識」忘失の恐れがある |
| 「知識」と「所持」を併用 | ● IC カードと暗証番号の併用<br>● ワンタイムパスワードトークンとパスワード（暗証番号）の併用<br>● SIM[9]カード（携帯電話／スマートフォンの固有番号）とパスワードの併用 | ● 「知識」と「所持」を併用することで、「知識」だけ、あるいは「所持」だけに頼るよりも安全性が高い | ● カードやトークン等が必要で運用コストが高い<br>● カードやトークン等の盗難･紛失の恐れがある<br>● 「知識」亡失の恐れがある |
| 「所持」を利用する手段 | ● IC カード<br>● USB トークン<br>● SIM カード（携帯電話／スマートフォンの固有番号） | ● 「知識」に頼らず、安全性を向上できる | ● カードやトークン等が必要で運用コストが高い<br>● カードやトークン等の盗難･紛失の恐れがある<br>● 正規の利用者でなくでも、何らかの手段（例えば窃盗や偽造）でカードやトークン等を「所持」することができれば、システムは正規の利用者と誤認する |

[9] Subscriber Identity Module Card。携帯電話等で使われている電話番号を特定するための固有の ID 番号が記録された IC カード

表 2　システムが正規の利用者かどうかを判断する認証手段（続）

| 認証手段の概要と具体例 | | 利点 | 欠点 |
|---|---|---|---|
| 「存在」を利用する手段 | ● バイオメトリクス認証（指紋、声紋、静脈等） | ● 「知識」や「所持」に頼らず、安全性を向上できる<br>● 偽造がかなり困難<br>● 盗難・紛失の恐れがない | ● 特別な装置が必要で、運用コストが高い<br>● システム・装置によって認証精度に大きなばらつきがある<br>● 認証データは本人固有の生体情報を基にして作られるため、万が一、認証データの漏えいや偽造が発生しても、認証データ自体を変えることができない |
| | ● リスクベース認証（行動パターン、キーボードを使う時の癖など） | ● 行動パターンや癖などをまねるのは難しい<br>● 完全に一致する行動パターンや癖が現れるのもかえって不自然と判断可能<br>● 盗難・紛失の恐れがない | ● 完全な利用者認証にはならない。“リスクベース”とは、行動パターンやキーボードを使う時の癖がいつもと違うことを検出した時に、“他人が利用しているかもしれない＝リスクの検知”と判断して、別の利用者認証を要求する、という意味<br>● 状態監視が常時必要なので、運用コストも比較的かかる |

表 2 に示すように、それぞれの認証手段には各々異なった利点と欠点がありますので、状況に応じた使い分けが必要です。

特に重要な情報を扱う場合には、利用者認証の信頼性を高める意味で、いくつかの認証手段を組み合わせることも有効です。一般に「多要素認証」と呼ばれ、なかでも 2 つの認証手段を組み合わせる場合を特に「二要素認証」といいます。「知識」と「所持」の併用なども二要素認証の一種です。

## 2.4.2.2　パスワードを使った利用者認証には細心の注意を払う

パスワード（知識）を使った利用者認証（パスワード認証）は、特別な装置が不要で非常に簡便であるため、広く使われています。例えば、端末ロック機能やアプリケーションの暗号化機能など、標準搭載された機能で使われています。

### パスワードを使った認証の最大の問題は「パスワードの安全性は決して高くない」

表 3 は、利用できる文字種類すべてを完全にランダムに選択して作ったパスワードを一つ一つ調べる全数探索により 1 日で解読しようとした際にかかるおおまかな想定攻撃コストを示しています。

ここでは、全数探索（暗号鍵の総数 $2^{56}$）でDES[10]を 1 日で解読するためのコストを約 250 万円と仮定します（コラム④参照）。また、パスワードを 1 つ検査するのとDESの暗号鍵を 1 つ検査するコストは同じであるとし、パスワードを求めるのに必要な計算量（検査する個数）が半分になればコス

[10] Data Encryption Standard。1977 年に米国政府標準暗号として定められた

トも半分、2 倍になればコストも 2 倍になるものとしています。

なお、解読条件や用意できる計算機環境、計算機の運用コストなど、多くの不確定要素があるため、実際のパスワードの解読コストを正確に算出することは非常に困難ですので、あくまで参考の一つとしてみてください。

**表 3　パスワード解読の想定コスト例**

| 利用する文字種類数と内訳 | | | | パスワード長 | | | |
|---|---|---|---|---|---|---|---|
| 種類数 | 数字 | 文字 | シンボル | 4 文字 | 8 文字 | 12 文字 | 16 文字 |
| 10 種 | 0–9 | なし | なし | 1 円未満<br>(計算量 : $2^{13.3}$) | 1 円未満<br>(計算量 : $2^{26.6}$) | 約 35 円<br>(計算量 : $2^{39.9}$) | 約 35 万円<br>(計算量 : $2^{53.2}$) |
| 36 種 | 0–9 | a–z | なし | 1 円未満<br>(計算量 : $2^{20.7}$) | 約 100 円<br>(計算量 : $2^{41.4}$) | 約 1.65 億円<br>(計算量 : $2^{62.0}$) | 約 276 兆円<br>(計算量 : $2^{82.7}$) |
| 62 種 | 0–9 | A–Z<br>a–z | なし | 1 円未満<br>(計算量 : $2^{23.8}$) | 約 7,500 円<br>(計算量 : $2^{47.6}$) | 約 1,120 億円<br>(計算量 : $2^{71.5}$) | 約 165 京円<br>(計算量 : $2^{95.3}$) |
| 94 種 | 0–9 | A–Z<br>a–z | !”#$%&’()=~\|-^`<br>¥{@[+*];:}<>?_,./ | 1 円未満<br>(計算量 : $2^{26.2}$) | 約 21 万円<br>(計算量 : $2^{52.4}$) | 約 16.5 兆円<br>(計算量 : $2^{78.7}$) | 約 129,000 京円<br>(計算量 : $2^{104.9}$) |

表 3 からわかることは、使う文字種類数の多少にかかわらず、パスワード長が短い場合にはパスワードを解読するコストはほとんどかからないということです。つまり、「1234」であろうが、「e$9_」であろうが、パスワード長が 4 文字である以上は本質的な安全性はほとんど違いません。

また、肩越しに覗き見る「ショルダーハッキング」やテンキー、キーボード、タッチパネルなどに付着する汚れ具合から入力位置が特定でき、入力した文字がわかることがあります。結果として、パスワード長が短い場合には、パスワードそのものがわかることにもつながります。

パスワード設定時に「パスワード長は 8 文字以上」「英数字・記号を混在させる」といった条件が与えられる場合がありますが、これは安全なパスワードを作らせるための最低要件を示したものといえます。

## パスワードをランダムに作って運用するのは難しい

表 3 を参考にするうえでもう一つ注意する必要があるのは、現実問題としてパスワードを忘れないようにするために、覚えやすいパスワードや規則的な変換ルールを使ったパスワードを実際に選ぶ傾向があることです。そのため、現実にはランダムに作られたパスワードにはなっていないため、パスワードの安全性は表 3 よりもはるかに低くなる場合が多いことに注意してください。

例えば、「passphrase」→「P@$$phr@59」、「World_Cup」→「vv0r1d_[up」なども一見すると使っている文字種類数が多く安全なように見えますが、よく知られている変換ルールを使っているため、比較的容易に推測可能なパスワードといえます。実際、辞書攻撃やレインボーテーブル攻撃といわれ

る手法を用いたパスワード解読ツールでは、多くの場合にパスワードがランダムに作られていないことを利用して、よく使われる単語や変換ルール、記憶しやすい文字列などを集めて効率よくパスワードを見つけ出しています（図 8）。

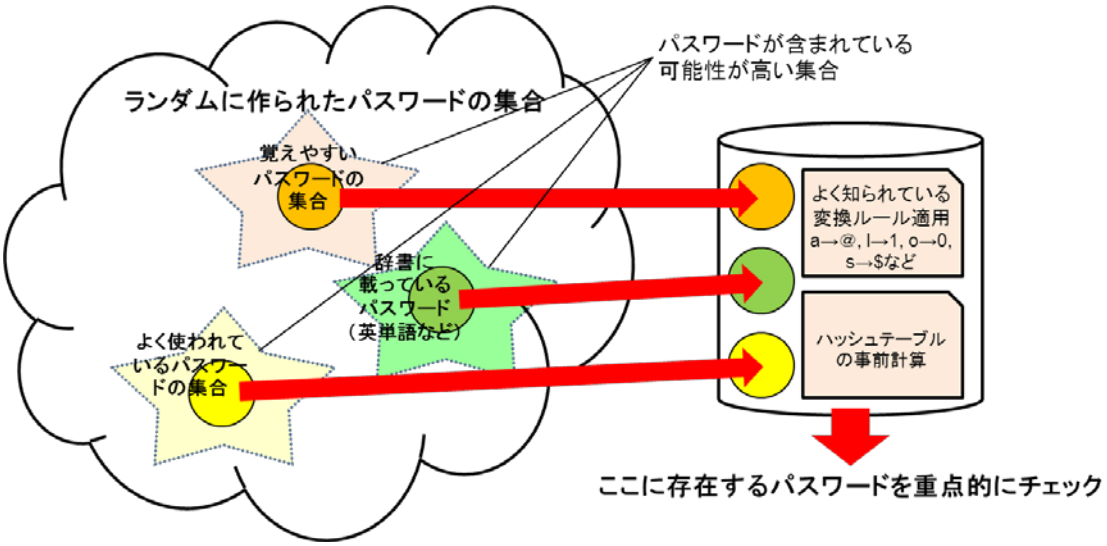



**図 8　パスワード解読ツールはやみくもにパスワードを探索するわけではない**

パスワード解読ツールとして、現実に「パスワードクラッカー」と呼ばれるソフトウェア（フリーソフトもあります）やクラウドサービス [11]さえも存在しています。

形式上、これらの解読ツールは「弱いパスワードであるかどうかをあらかじめ判定」するために実際にパスワードを解読してみせることを目的としています。しかし、現実のパスワードを見つけ出すためにも利用できることは明らかです。

## パスワードを使った認証を安全に使うには

このように、**記憶できるようなパスワードだけで十分な安全性を確保することはかなり困難**です。

そのため、パスワードである程度の安全性を確保しようとするならば、完全ロック機能（あらかじめ設定した回数以上のパスワード認証誤り後は、特別な解除処理をしない限り以後のパスワードの入力を受け付けない）、またはロックアウト期間設定（一定時間パスワードの入力を受け付けない）を有効にして、**パスワード認証の失敗回数に制限を加えることなど、別の対策との併用が必要**です。場合によっては、パスワード認証以外の対策を考慮することも検討に入れるべきです。

また、少しでも強いパスワードを作りたいのであれば**「パスワード強度チェッカー」**を利用して、安全と判定されたものを使ってください。

「パスワード強度チェッカー」は作ったパスワードがどの程度複雑であるかを数段階のレベルで判定してくれるものです。アプリケーションなどに付属してある場合のほか、例えば、マイクロソフト

[11] あるサイトでは 20 分あたり$17 で利用可能

のサイト[12]でも（非公式ですが）提供されています。

## 【コラム④】DES はどのくらいのコストで解読できるか

DES (Data Encryption Standard)は、1977 年に米国政府標準暗号として定められた後、2005 年に正式に廃止されるまで世界中で広く利用されてきた共通鍵暗号です。DES の特筆すべき点は、それまで暗号といえば軍事・外交用の暗号アルゴリズムであったものを、政府や民間が利用する暗号アルゴリズムとして使えるようにしたことです。そのために、米国政府は政府標準暗号として世界で初めて暗号アルゴリズムの仕様を公開しました。

これによって、実用的には仕様書さえ入手できれば、誰もが DES を実装して利用できるようになり、多くの暗号製品が作られました。また、学術的には、秘密裏に行われていた暗号解読や暗号設計などの様々な暗号研究が公に行われる契機となりました。

DES の安全性について、共通鍵暗号のもっとも基本的な安全性の評価指標は「取り得るすべての暗号鍵を 1 つずつしらみつぶしに検査をして正しい暗号鍵を見つけ出す手法」です。鍵全数探索法と呼ばれ、原理的にはどのような暗号アルゴリズムにも適用できる暗号解読法です。したがって、鍵全数探索法に対する安全性は、実用的な時間内にすべての候補となる暗号鍵を検査できるだけの計算能力が存在するか否かという点だけで決まります。

例えば、DES の鍵長は 56 ビットであり、鍵の総数は $2^{56}$ 個=約 7 京個あります。

そこで、実際に鍵全数探索法によってどれだけの時間で DES の正しい暗号鍵が求められるかを競う懸賞金付き解読コンテスト DES Challenge が 1997 年から 1999 年にかけて合計 4 回実施されました。結果としては、世界中の多くのボランティアの協力の下、いずれの回でも正しい暗号鍵を見つけ出すことに成功しました。特に、第 4 回 DES Challenge では 1 日を切る時間で正しい暗号鍵を見つけ出しています。

単独の DES 専用解読装置としては、1998 年の第 3 回 DES Challenge の時に初めて DES Cracker が作成されました。DES Cracker では、DES の暗号鍵を 1 日当たり約 $2^{52.8}$ 個検査する能力があり、開発費は$250,000 と言われています（1 日ですべての暗号鍵を検査しようとすれば約 10 台の DES Cracker が必要）。

その後も計算機能力は年々性能向上するため、実際に 2007 年に開発された COPACOBANA は 1 日当たり約 $2^{52.3}$ 個の検査能力があり、開発費が約$10,000 と言われています（1 日ですべての暗号鍵を検査しようとすれば約 13 台の COPACOBANA が必要）。

そこで、表 3 の想定コスト例を作成するにあたっては、18～24 ヶ月で性能が 2 倍になったりコストが半減したりする経験則（ムーアの法則）を考慮し、現時点（2012 年）での解読装置の能力は COPACOBANA の約 4～5 倍になっていると仮定しました。

[12] https://www.microsoft.com/ja-jp/security/pc-security/password-checker.aspx

### 2.4.2.3　バイオメトリクス認証で注意すべきこと

バイオメトリクス認証（生体認証）は、指紋、声紋、静脈などといった正規の利用者自身の身体的特徴を使って利用者認証を行うことから、一つ一つのパスワードが正しいパスワードかどうかを全数的に調べていくパスワード解読ツールのような攻撃方法は、バイオメトリクス認証には効きません。また、記憶の亡失や、IC カードや USB トークンなどといった利用者認証用トークンの紛失といったリスクを考慮しなくてよい点もバイオメトリクス認証の長所として挙げられます。

このことから、一般にはパスワード認証などよりも安全性が高い認証方式と受け取られています。

**バイオメトリクス認証での認証精度の違い**

しかし、バイオメトリクス認証で注意をしなければならないのは、**「認証精度がシステム・製品や設定によって大きく異なる」**という点です。

専門的には「他人受入率（FAR[13]）」と「本人拒否率（FRR[14]）」と呼ばれる指標で認証精度が表されます。簡単に言えば、他人受入率は「システムが他人を正規の利用者であると誤認する確率」、本人拒否率は「システムが正規の利用者を他人であると誤認する確率」です。例えば、FAR 0.01%、FRR 0.1%であれば、1 万人に 1 人ぐらいの確率で他人を正規の利用者と誤認し、1000 回に 1 回ぐらいの確率で正規の利用者でも認証に失敗する、ということを意味します。一般に、他人受入率を下げようとすると本人拒否率が上がり、本人拒否率を下げようとすると他人受入率が上がる特性があります。

安全性の面からは他人受入率が低いほどいいのは当然ですが、正規の利用者本人さえ拒否されるようになると利便性が低下します。逆に、本人拒否率を低くして利便性を上げると、他人を正規の利用者と誤認する可能性が増え、安全性の問題につながります。

つまり、どのようなシステム・製品であれ、そこで使われているバイオメトリクス認証は**「安全性と利便性のトレードオフを考慮して認証精度が設定」**されていることになります。デフォルトで設定されている認証精度は、あくまで「そのシステム・製品の多くの購入者にとって安全性と利便性の適度なバランスが取れているだろう」とその製品やシステムを製造しているメーカーが判断したレベルにすぎません。どちらかといえば利便性のほうが重要視されている可能性すらあります。

例えば、Android での「顔認証（フェイスアンロック）の認証精度はセキュリティレベル低」としています。「パスワード認証がセキュリティレベル高」としていることから見ても、安全性よりも利便性を重視した認証精度に設定していることが明らかです。

このように、バイオメトリクス認証を採用する際には、**その製品やシステムに設定されている認証精度（特に他人受入率 FAR）を必ず確認**してください。そして、デフォルトの認証精度では安全性のレベルが十分でない（他人受入率が高い）のであれば、他人受入率を下げるような認証精度の設定に変更してください。

---

[13] False Accept Rate
[14] False Reject Rate

もし、**必要な安全性のレベルにまで他人受入率を下げることができないのであれば、そのバイオメトリクス認証は使わないか、別の認証手段との併用が必要**です。

## バイオメトリクス認証が実質的に機能回避されないように注意

ノートパソコンや USB メモリなどに付属しているバイオメトリクス認証装置では、例えば、指紋などの認識ができなかった場合の救済用としてパスワード入力を行って利用者認証ができるようになっているものが多く存在します。これは、仮にバイオメトリクス認証が通らなくても、救済用のパスワード認証のほうを通りさえすれば、ノートパソコンや USB メモリにアクセスできるようにするためです。

逆の見方をすれば、せっかくバイオメトリクス認証を用いているにもかかわらず、**救済用のパスワードによる認証とバイオメトリクス認証のどちらか低い方の安全性になってしまう**ことに注意する必要があります（図 9）。つまり、救済用のパスバードの安全性が不十分な場合、**実質的な安全性はパスワード認証そのものになる**ということです。

決して「バイオメトリクス認証とパスワード認証の二要素認証である」と誤解しないでください。

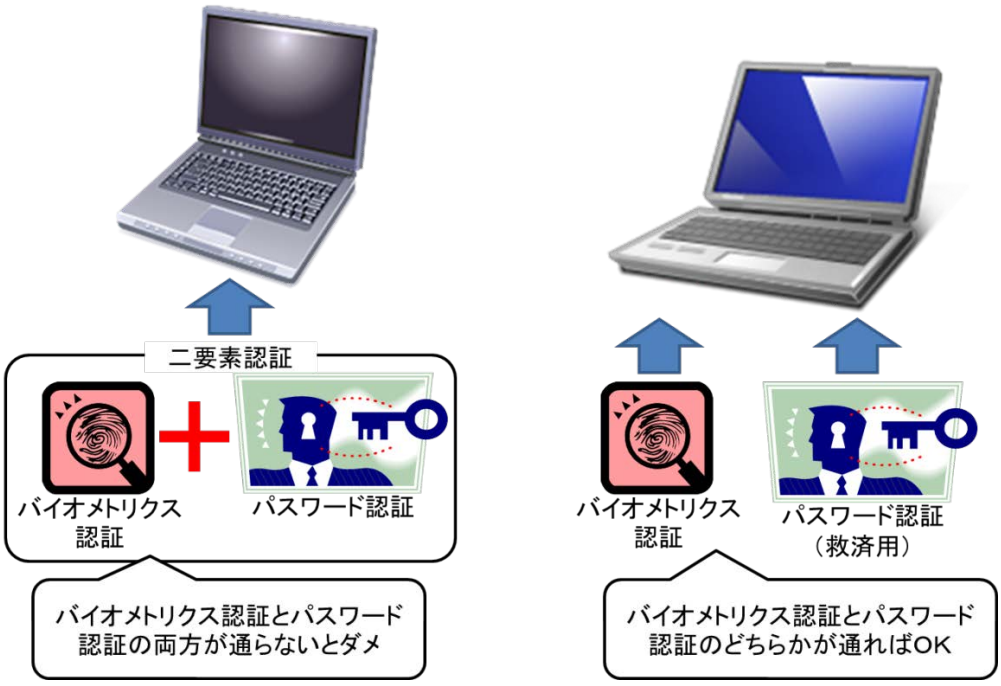



図 9　二要素認証と救済用におけるパスワード認証の位置づけの違い

**救済用のパスワードはあくまで「非常時にだけ使えればよい」との位置づけ**を明確にし、通常時の利用は想定しない、極めて強固なパスワード（完全にランダムに選ばれた長い文字列）、パスワード認証連続失敗時の端末ロックを設定するなどの対応が必要です。

この場合、救済用のパスワードを覚える必要は全くありません。非常時にだけ取り出せる、安全な場所に救済用のパスワードを記録保管しておけば十分です。間違っても、ノートパソコンや USB メモリなどと一緒に救済用のパスワードを携帯しないことだけ徹底してください。

## 【コラム⑤】指紋認証をだます方法 ～“グミ指”を知っていますか？～

指紋は「生涯不変」「万人不同」と言われており、個人識別の手法としては信頼性が高いものです。実際、犯罪捜査などでも使われていますし、バイオメトリクス認証として当初から指紋認証がもっとも利用されています。

それにも拘わらず、なぜ指紋認証での他人受入率がゼロパーセントにならないのでしょうか。その理由は、指紋認証が、指紋全体を隅々までくまなく調べて個人を識別しているわけではないことに起因します。

一般に、指紋認証では、以下の手順で認証を行います。

① 指紋センサーで指紋の画像を撮影
② 撮影した画像から指紋の隆線（線のように見える模様）を抽出
③ 抽出した稜線を分析して、隆線が分岐する場所（分岐点）や隆線が途切れる場所（端点）など、特徴的な場所（特徴点）を特定（図 10）
④ テンプレート [15]として登録されている利用者の特徴点と③の特徴点が一致するかを判定し、高い一致度（多くの場合、十数か所の特徴点が一致）を満たせば利用者本人と認証

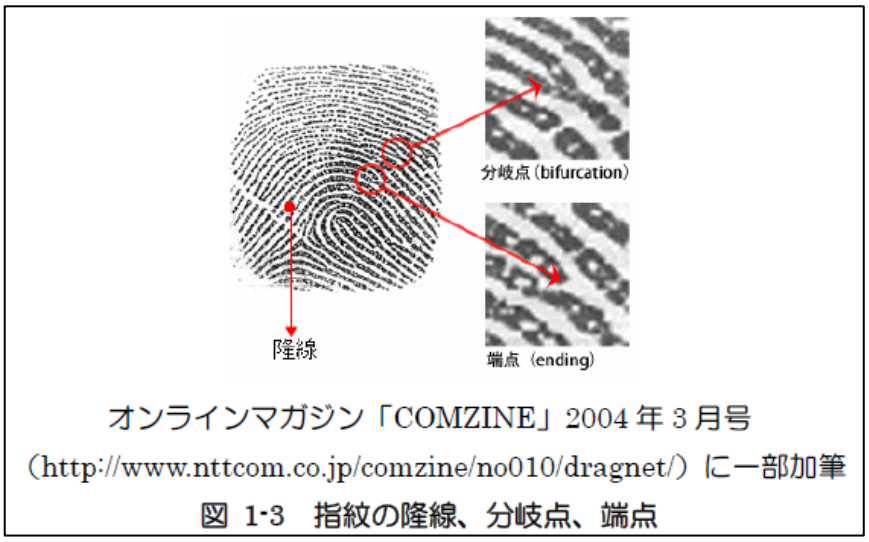



**図 10 指紋の隆線、分岐点、端点 [16]**

[15] 利用者の指紋として始めに登録された指紋認証の基準となる情報のこと
[16] IPA「生体認証導入・運用の手引き」より引用。
http://www.ipa.go.jp/security/fy24/reports/bio_sec/documents/bio_guide_24.pdf

指紋が登録できなかったり認証できなかったりという場合には、その多くが「②の段階で稜線がうまく抽出できず、③の段階で必要な量の特徴点が見つけ出せない」ことに原因があります。

一方、他人受入率の高低は「④の段階での一致度をどの程度必要とするか」に依存しています。具体的には、必要とする一致度を高くすれば、多くの特徴点でテンプレートとして登録されている利用者の特徴点と一致する必要があるため、他人受入率を低くできます。しかし、同時にわずかなズレやかすれなどで特徴点がうまく取れなかった場合には、必要な数の特徴点が揃わず、正規の利用者でも認証に失敗することになります。反対に、少ない一致度でもよいとすれば、テンプレートとして登録されている利用者の特徴点とたまたま数か所が一致するだけで、利用者本人と誤認してしまうことになります。

適切な他人受入率が設定されていれば、端末に登録されている利用者の指紋の特徴点と非常によく似た指紋の特徴点を持つ第三者が数千人に一人いる状態であっても、その人が偶然その端末を拾得して指紋認証をパスするといったことが起きる可能性は現実にはかなり低いといえるでしょう。

一方で、攻撃者の都合がよい特徴点を利用者のテンプレートとしてシステムに誤認させて登録したり、あらかじめ登録されている利用者の特徴点を忠実に再現する方法があれば、指紋認証をだますことができます。有名なところでは、指紋を転写した基盤にゼラチンを流し込んで固めて作った「グミ指」や登録した利用者の指紋が表面についた「指紋テープ」を使って、実際に指紋認証をだますことができた事例が報告されています。

なお、IPAでは、指紋認証のほか、静脈認証、虹彩認証など、様々なバイオメトリクス認証についての調査検討を行い、生体認証利用における注意点と利用事例を取りまとめた「生体認証導入・運用の手引き」を公開[17]しています。

バイオメトリクス認証を本格的に導入する際には、こちらの手引きも参照してください。

[17] http://www.ipa.go.jp/security/fy24/reports/bio_sec/documents/bio_guide_24.pdf

### 2.4.3　端末が信頼できる状態で暗号製品を使う

#### 2.4.3.1　セキュリティパッチを適用することは必須

暗号アルゴリズム以外の脆弱性を使った攻撃を完全に防ぐことは容易ではありませんが、暗号アルゴリズム自体が解読されたわけではありませんので、発見された脆弱性に対して実装上の修正を施したり、運用でうまく回避することによって、暗号化された情報の内容（平文）が見られることを防ぐことができます。

そこで、脆弱性が発見されて対策が必要であると判断されると、通常、暗号製品を出しているベンダからその脆弱性を修正するためのセキュリティパッチが公開されます。つまり、攻撃者がそういった脆弱性を使って攻撃できるようになったときからその脆弱性を修正するセキュリティパッチが適用されるまでの期間が脅威にさらされている期間といえます。

暗号製品に限った話ではありませんが、**セキュリティパッチが公開されたらできるだけ早く適用**するようにと言われる理由も、その点にあります。

もう一つの典型的な攻撃手法として、中間者攻撃（Man-in-the-middle 攻撃）と呼ばれる手法が使われます。この手法では、攻撃のターゲットにされた利用者とその利用者の通信相手との間に攻撃者が“能動的”に入り込んで通信データに細工することが必要なため、両者の通信路中に物理的に入り込むケースのほか、利用者の端末にウイルス感染させて通信相手自体を攻撃者に設定させることで必要な情報を攻撃者が得るケースが想定されます。

その点からも、**ウイルス対策を徹底し、マルウェア・ウイルスに感染しないことも必要**です。

このほか、**使っている暗号製品のバージョンにも注意**してください。

当該製品を出しているベンダによるサポートが切れているバージョンの製品では、たとえ脆弱性が見つかったとしても、セキュリティパッチが提供されることは期待できません。また、サポートが切れていなかったとしても、新しいバージョンのものほど脆弱性に対する対策が多く取り込まれて初めから安全性が高まっている一方、古いバージョンのものほど新しい安全な仕組みが使えず安全性が低いまま、といったケースが多いことにも注意してください。

#### 2.4.3.2　信頼できる暗号製品を使う ～セキュリティ認証制度～

基本的に暗号化処理の動作は不可視であることから、**暗号製品の信頼性は、事実上、製造会社・販売会社に全面的に依存**しているといっても過言ではありません。

例えば、「安全性が高い米国政府標準暗号 AES で暗号化しているから安全である」と謳っていても、実際に AES が正しく実装されているのか、あるいは暗号鍵が安全に生成・保管されているのか、といった暗号化処理の根幹に関わることですら、利用者がその安全性や妥当性を確認することはほとんど不可能です。

そこで、暗号製品として安全に利用できることを中立的かつ第三者的に確認・検証し、安全性が確認されたものに対してお墨付きを与える「セキュリティ認証制度」が作られています。

具体的には、「暗号モジュール認証制度（CMVP 認証, JCMVP 認証)」と「コモンクライテリア（CC）認証制度（ISO/IEC 15408 認証、JISEC 認証)」があり、それらの認証を取得しているかどうかによって、暗号製品としての安全性が第三者検証されたものであるかどうかを利用者が容易に判断することができます。

機密度の高い情報の持ち運びなどの利用が想定されている場合や暗号製品の選択に迷った時などでは、セキュリティ認証を取得した暗号製品のなかから選ぶということも一つの有力な考え方になります。

## 【コラム⑥】セキュリティ認証制度とは

- **暗号モジュール認証制度（CMVP[18]認証, JCMVP[19]認証）:**

**暗号化処理で必要な暗号アルゴリズムが正しく実装され、かつ安全に動作することを確認**する認証制度です。CMVP/JCMVP 認証取得製品には、図 11 のようなロゴが付けられています。

北米（米国及びカナダ）ではCMVP認証もしくはFIPS[20] 140-2 認証と呼ばれています。1994 年から施行されており、CMVP認証製品を採用することが米国政府の調達条件になっています。

日本では、JCMVP 認証として 2007 年から正式運用が開始されました。


**図 11　暗号モジュール認証ロゴ（左：CMVP 認証、右：JCMVP 認証）**

CMVP/JCMVP 認証では、暗号製品全体ではなく、暗号化処理を行う部分（暗号モジュール）に特化して安全性の検証が行われます。暗号モジュールに対する解読攻撃などへの耐性を含めた安全性の強度検証度合いに応じて、Lev 1 から Lev 4 の 4 段階で判定され、レベルが上がるほど高い安全性を有します。例えば Lev 4 なら軍用でも利用可能なレベルです。

なお、検証される暗号アルゴリズムはあらかじめ決められており、CMVP認証では米国政府標

[18] Cryptographic Module Validation Program
[19] 暗号モジュール試験及び認証制度：Japan Cryptographic Module Validation Program。https://www.ipa.go.jp/security/jcmvp/
[20] Federal Information Processing Standard

準暗号のみ、JCMVP認証ではセキュリティ機能として承認された暗号アルゴリズム [21]のみが認証対象となっています。つまり、CMVP/JCMVP認証取得製品に搭載されている暗号アルゴリズムであっても、認証対象以外の暗号アルゴリズムは検証されていないことに注意してください。

- **コモンクライテリア（CC: Common Criteria）認証制度（ISO/IEC 15408 認証、JISEC[22]認証）:**

暗号製品・システムに搭載される**セキュリティ機能が適切かつ確実に実装されていることを確認**する認証制度です。セキュリティ評価基準がISO/IEC[23] 15408 で規格化されており、これに基づいて認証されます。現在では、日本を含む 16 カ国でこの認証制度が作られており、そのいずれかの国で取得したCC認証はCC承認アレンジメント（CCRA[24]）に基づき全 26 カ国でその効力を有します。例えば、米国政府では、暗号化ストレージとして、ハードディスクのフルディスク暗号製品とUSBメモリの暗号製品に対して、共通のCC認証要求仕様 [25]（PP: プロテクションプロファイル）を定めていますので、このPPに基づいて米国でCC認証を取得した暗号製品は、日本でもCC認証取得済み暗号製品として販売できます。

CC 認証取得製品には、図 12 のようなロゴが付けられています。


**図 12　CC 認証ロゴ（左：CC 認証、中：CCRA に基づく認証、右：JISEC 認証）**

CC 認証では、暗号製品全体として、どのような脅威に対抗するものであるのか、またその脅威に対して安全であるようにするために必要なセキュリティ機能をどのように選択し、適切かつ確実に実装しているのか、についての実装上の妥当性検証が行われます。必要なセキュリティ機能がどの程度適切かつ確実に実装されているかの検証度合いに応じて、EAL 1 から EAL 7 の 7 段階で判定され、EAL が大きいほど様々な観点から実装上の妥当性が検証されます。

なお、EAL は実装上の妥当性の検証レベルを表したものであり、安全性を直接表したものではありません。また、暗号製品に搭載される暗号アルゴリズムの安全性自体は認証対象にはなっていないことに注意が必要です。どのような暗号アルゴリズムであれ、実装されている暗号アルゴリズムが想定されている脅威に対して対抗できるように適切かつ確実に実装されているか、という視点で認証されます。

---

[21] 詳細は、http://www.ipa.go.jp/security/jcmvp/algorithm.html を参照
[22] IT セキュリティ評価及び認証制度：Japan Information Technology Security Evaluation and Certification Scheme。https://www.ipa.go.jp/security/jisec/index.html
[23] 国際標準化機構／国際電気標準会議：International Organization for Standardization／International Electrotechnical Commission
[24] Common Criteria Recognition Arrangement
[25] 暗号製品ごとに想定する脅威や対抗措置の水準が異なることを防ぐために、暗号製品の分野ごとにあらかじめ対処すべき脅威や対抗措置の最低基準を共通的に取りまとめた要求仕様書 https://www.ipa.go.jp/security/publications/niap/spp-jp/index.html に米国政府のプロテクションプロファイルの日本語訳が掲載されている

# 3. 暗号化による情報漏えい対策の実施方法 ～ベースライン対策～

本章では、暗号化によって情報を保護するうえで、具体的にどんな対策をすれば何が守られ、何が守れないかを簡単に説明します。なお、ここで示す**実施対策はあくまで対策のベースライン（最低水準）**です。**対策水準を上げる必要性があるかどうかを必ず検討**するようにしてください。

## 3.1　暗号化を行う方法について

暗号化を行う方法として、大きく 2 つあります。一つは個々のファイル単位に暗号化を行う**「ファイル暗号化」**であり、もう一つはドライブストレージ（ハードディスクや SSD など）全体あるいはフォルダのような特定領域ごとに一括して暗号化を行う**「領域暗号化」**です。

両者には異なった利点、特徴と注意すべき点がありますので、状況や用途によって使い分ける必要があります。場合によっては、併用することも考慮すべきです。

### （ア）ファイルの暗号化による保護

アプリケーションの暗号化機能などを利用して、ファイル単位で個別に暗号化を行います[26]。そのファイルにアクセスする権限がある利用者だけが元の情報（平文）を見ることができます。多くの場合、ファイルにアクセスする権限がある利用者であるかどうかは、正しいパスワードを知っているかどうかで判断されます。

この方法は、端末・媒体などの制限を受けないので、**使う端末・媒体が特定されていないケース（例えばメール送信や複数端末での共有など）で特に有効**です。

＜メリット＞

- アプリケーションの基本機能として装備されていることも多く、すぐに利用可能。ファイル暗号化ソフトを利用すれば、より細かい設定も可能
- 端末・媒体外にデータを持ち運んでも（例えば、他媒体へのコピー、メール添付、ファイル共有サーバへのアップロードなど）暗号化が解除されることはない
- 端末・媒体自体は利用できる正規の利用者であっても、ファイルにアクセスする権限がなければ元の情報（平文）を見ることができない

＜注意すべき点＞

- 自動的に暗号化されないのがほとんどであるので、**暗号化のし忘れが起きやすい**
- パスワードしか使えないことが多い
- ファイルを入手できて、かつ**パスワードがわかれば誰でも元の情報を見ることができる**
- 一般にはパスワードを忘れると、その暗号化ファイルを復号する手段がなくなる

[26] Windows ではファイルの暗号化に EFS (Encryption File System)も利用可能である。ただし、EFS でファイル暗号化した場合は、例外的に、「(イ) ドライブ（全記憶領域）／フォルダ（特定領域）の暗号化による保護」に記載した特徴をもつことに注意すること

### （イ）ドライブ（全記憶領域）／フォルダ（特定領域）の暗号化による保護

OSの暗号化機能や専用の暗号化ソフトを利用して、ドライブストレージ全体（ハードディスクやSSD[27]などの全記憶領域）、もしくはフォルダ（特定領域）全体の暗号化を行うことによって、端末内に保存される全データ、もしくは特定領域内の全データを正規の利用者以外から保護します。正規の利用者であるかどうかは、端末・媒体を起動させ、操作可能な状態にすることができるかどうかで判断されます。

この方法は、**利用する端末・媒体が限定されており、それらを介してのみ情報の持ち運びをするケースで特に有効**です。

＜メリット＞

- 暗号化対象領域ではデータは自動的に暗号化されるため、暗号化のし忘れがない（暗号化を意識する必要がない）
- 端末・可搬媒体（USB メモリなど）を起動させることができなければ、暗号化対象領域の全データが保護される
- ドライブストレージを別端末に付け替えても暗号化対象領域にはアクセスできない
- コストをかければ、端末・媒体の起動や端末ロックの解除に必要な認証をパスワードより強固なものにすることも可能（例えば、バイオメトリクス認証、トークン認証）

＜注意すべき点＞

- デフォルトでは設定がオフになっているので、設定をオンにする準備が必要
- 正規の利用者でなくても、**端末・可搬媒体を起動させ、操作可能な状態にすることができれば、完全に無防備**になる（自動的に暗号化データへのアクセス権が付与され、透過的に元の情報（平文）を見ることができる）。例えば、ログインしたまま放置された PC や安易なログインパスワードを使った PC などでは、正規の利用者でなくても端末・可搬媒体を操作可能な状態にすることができる
- **端末・媒体外にデータを持ち運ぶ（例えば、他媒体へのコピー、メール添付、ファイル共有サーバへのアップロードなど）際に、暗号化が自動解除**され、元の情報（平文）のままの形で持ち出される。ウイルス感染などによる情報流出の場合も例外ではない
- ドライブストレージ全体の暗号化をしていたとしても、個別に設定しない限り、外部メディア（スマートフォンに挿入した SD カードなど）内の情報については暗号化されない
- 緊急時回復用の設定をしないで、端末・可搬媒体を起動させ、操作可能な状態にすることができなくなると、暗号化領域の全データへのアクセス手段が完全に失われる

[27] Solid State Drive。半導体メモリ（RAM やフラッシュメモリ）と使った記憶装置

## 3.2　情報価値レベルとベースライン対策の考え方について

情報を持ち運ぶことは、外部でも自由に情報が利用できる利便性を向上させる一方で、情報漏えいリスクも高めることになります。しかし、普段から活用しているお財布を大きな金庫にしまわないのと同じように、情報漏えいリスクと利便性のトレードオフを考慮しない高度な対策を一律に採用することは、著しい業務効率の低下を招いたり、費用対効果を悪化させたりする恐れがあります。

ここでは、持ち運ぶ際の情報漏えいリスクの多くが紛失・盗難であることに鑑み、端末や可搬媒体（USB メモリなど）を活用して持ち運ばざるを得ない情報を、情報漏えい時の影響度合いに応じて情報の価値レベル（4 レベル）に分け、最低限守るべき保護対策水準の目安とする考え方を示します（表 4）。

なお、代表例はあくまでも参考であり、常にその情報価値レベルを持つというわけではありません。**どの情報価値レベルに該当するかは自らの業務内容や情報の重要性、情報漏えい時の影響度の範囲（例えば影響を受ける人数）等を考慮のうえ、自らの責任で適切に判断する必要**があります。

また、情報価値レベルに応じて、最低限とるべき対策についての考え方を合わせて示します。

これらの対策をとった場合に**「どういった効果が期待できるのか」を必ず確認**してください。当該対策の効果では不十分、という場合には、対策レベルを上げるなどの対応をしてください。

**表 4　情報価値レベルとベースライン対策の考え方**

| | | |
|---|---|---|
| 情報価値レベル 4 の考え方 | | 漏えいさせた場合には、重大な悪影響をもたらし、信用棄損のみならず、経営的にも多大な損害が発生する可能性が高い情報 |
| | 代表例 | ● 本人を特定でき、経済的損失を引き起こす（＝犯罪に利用される）可能性がある情報（オンラインバンキング・オンラインショッピングなどで必要となる情報の組み合わせ、等）<br>● 本人を特定でき、著しい精神的苦痛を与える（＝差別を誘発する）可能性がある情報（基本的人権に関わるような情報、等）<br>● 業務秘密として特に厳重に管理すべき情報（経営機密情報、等）<br>● 法律・契約等により保護されるべき情報<br>● その他、外部に持ち運ぶ必要性に乏しい情報 |
| 対策レベル 4 の考え方 | | 正規の利用者以外は暗号鍵が事実上利用できない極めて強固な認証と暗号化を併用することにより、暗号解読以外の手段で元の情報（平文）を見ることを極めて困難にする |
| | 期待できる対策効果 | 暗号解読に必要な計算能力、コストが非現実的である限り、元の情報（平文）が見られる可能性はほとんどない |

表 4　情報価値レベルとベースライン対策の考え方（続）

| | | |
|---|---|---|
| 情報価値レベル 3 の考え方 | | 漏えいさせた場合には、重大な悪影響をもたらす可能性があり、信用棄損の他、場合によっては経営的にも損害が発生する可能性がある情報 |
| | 代表例 | ● 本人と個人識別情報を結び付ける情報（氏名と社員番号や会員番号などとの組み合わせ、等）<br>● 本人を特定でき、かつ本人に付随する公開されていない情報（家族の構成情報、資産情報、疾病歴、等）<br>● 本人を特定でき、生活様式（行動パターン）が明らかになる可能性がある情報（学業成績、購入履歴情報、等）<br>● 業務秘密として管理すべき情報（研究開発成果、営業情報、社外秘情報、等） |
| 対策レベル 3 の考え方 | | 利用者認証の厳格化と暗号化による対策を多重化することにより、情報漏えいの可能性を大幅に低減する |
| | 期待できる対策効果 | 端末・可搬媒体等に入っているデータに対して、対策を破るコストが情報価値を大きく上回るようにすることで、元の情報（平文）を見てもメリットがないと感じさせ、情報を見ようと努力するモチベーションを大きく低下させる |
| 情報価値レベル 2 の考え方 | | 漏えいさせた場合でも、重大な悪影響が生じる可能性は小さいが、企業倫理上、安易に見られることは避けたい情報 |
| | 代表例 | ● 本人を特定するための公開情報ではあるが、本人が公開範囲を一定程度コントロールできる情報（電話帳、個人の公開情報の組み合わせ、等）<br>● 本人が特定されない形での生活様式（行動パターン）が明らかになる可能性がある情報（アンケート調査結果、等）<br>● 無関係の人に対しては開示する必要性がない情報（関係者外秘情報、等）<br>● いずれ公開される情報であるが、その時点では公開されていない情報（公開前の講演資料、等） |
| 対策レベル 2 の考え方 | | パスワード解読ツールなどの比較的入手が容易な手段を使うぐらいでは情報が簡単には見られないようにする |
| | 期待できる対策効果 | 端末・可搬媒体等を偶然入手（例：拾得）した人がその中の情報を見ようと努力することをあきらめさせる |
| 情報価値レベル 1 の考え方 | | 上記以外の情報 |
| | 代表例 | ● 本人が特定されない形での個人識別情報（会員番号のみ、等）<br>● 本人が特定されない形での本人に付随する情報（生年月日のみ、職業のみ、等） |
| 対策レベル 1 の考え方 | | 情報を見ようとする意欲自体を失わせる（心理的障壁を作る） |
| | 期待できる対策効果 | 端末・可搬媒体等を偶然入手（例：拾得）した人が興味本位でその中の情報を見ようとすることをあきらめさせる |

## 3.3　端末・可搬媒体に対するベースライン対策

ノートパソコンのような端末に情報を入れるのか、USB メモリのような可搬媒体に情報を入れるのか、によっても取り得る対策が異なります。

ここでは、「(i) ノートパソコン・タブレット」「(ii) 携帯電話・スマートフォン」「(iii) USB メモリ・外付けドライブストレージ」の 3 種類に分けて、対策のベースラインを示します（表 5)。どの対策レベルを選択するかについては、3.2 節の情報価値レベルとベースライン対策の考え方を参考にしてください。

なお、**ここでの対策はあくまでベースライン（最低水準）ですので、情報価値や利用環境によって許容可能な情報漏えいリスクを自ら判断**して、リスクに応じた費用対効果の高い対策を導入することが必要なことにも注意してください。

また、暗号化関係以外のセキュリティ対策（最新のセキュリティパッチの適用、ウイルス対策の実施など）は、確実に実施されていることを前提とします。例えば、**端末・媒体を介した情報の持ち運びではなく、ウイルス感染や不正アクセスによる情報流出の場合、ファイル暗号化以外では情報の保護ができません**。

対策例に挙げる項目において、「実施すべき項目」は、最低水準の安全性を保つために**すべてを必須的に実施すべき項目**です。**すべての項目が実施できない場合、その対策レベルは達成できない**と考えてください。また、「実施が望ましい項目」は、一つでも二つでも**実施可能なものについて対策を行うことが望ましい項目**を表しています。

なお、「A.1 (実践編-3) 端末ロックによる利用者認証の有効化」の「A.1 (実践編-3)」は実践編 I.での「A.1」の対策項目（実践編 3 ページ）であることを示しています。

参考までに、実践編は以下の内容のものをまとめていますので、必要に応じて、実践編も参照してください。

- 実践編 I：情報保護対策の具体的手法例
- 実践編 II：ユースケースと対策例
- 実践編 III：代表的な製品の具体的な設定方法の実例（対象は以下の通り）
  - ① Windows 7, Windows 8 での設定方法一例
    - ✧ A.1 端末ロックによる利用者認証の有効化（利用者認証の設定方法）
    - ✧ A.2 端末ロックによる利用者認証の安全性強化 (利用者認証失敗時の動作設定方法)
    - ✧ C.1 ドライブ／フォルダの暗号化設定と端末ロックによる利用者認証の有効化（ドライブ暗号化（BitLocker）の設定方法、フォルダ暗号化（EFS[28] を利用）の設定方法)

[28] Encrypting File System

② iOS 6 での設定方法一例

- ✧ A.1 端末ロックによる利用者認証の有効化（利用者認証の設定方法）
- ✧ A.2 端末ロックによる利用者認証の安全性強化
- ✧ C.1 ドライブ／フォルダの暗号化設定と端末ロックによる利用者認証の有効化

③ Android 4.x での設定方法一例

- ✧ A.1 端末ロックによる利用者認証の有効化（利用者認証の設定方法）
- ✧ A.2 端末ロックによる利用者認証の安全性強化
- ✧ C.1 ドライブ／フォルダの暗号化設定と端末ロックによる利用者認証の有効化（スマートフォン端末・タブレット端末での暗号化設定方法）

④ Microsoft Office（Word, Excel, Powerpoint）での設定方法一例

- ✧ B.1 ファイルへの暗号化設定の有効化（保存方法）

⑤ Adobe Acrobat（PDF ファイル）での設定方法一例

- ✧ B.1 ファイルへの暗号化設定の有効化（保存方法）

⑥ Imation[29]指紋認証付USBメモリでの設定方法一例

- ✧ C.3 端末起動時および端末ロックによる利用者認証の安全性強化（バイオメトリクス認証設定、回復用パスワード（マスターパスワード）設定）
  ※「C.1 ドライブ／フォルダの暗号化設定と端末ロックによる利用者認証の有効化」の設定を含む

[29] 指紋認証付 USB メモリは各社から色々な製品が出ているが、セキュリティ認証規格（2.4.3.2 節参照）を取得している製品は多くない。ここでは、CMVP 認証を取得している製品例として Imation 社の製品を取り上げた

**表 5　ベースライン対策例**

| 媒体種類 | 対策レベル | | 対策想定例 | 参照 |
|---|---|---|---|---|
| (i) ノートパソコン・タブレット | 対策レベル 1 | 1-1 | ● ノートパソコンやタブレットの利用者認証の実施 | P.36 |
| | 対策レベル 2 | 2-1 | ● ノートパソコンやタブレット内のドライブ暗号化の実施 | P.36 |
| | | 2-2 | ● ノートパソコンやタブレットの利用者認証の実施とファイル暗号化の併用 | P.36 |
| | 対策レベル 3 | 3-1 | ● 指紋認証機能付き高セキュリティノートパソコン内のドライブ暗号化の実施<br>● ノートパソコン内のドライブ暗号化と利用者認証用 USB トークンの併用<br>● タブレット内のドライブ暗号化とリモートワイプ設定の併用 | P.37 |
| | | 3-2 | ● ノートパソコンやタブレット内のドライブ暗号化とファイル暗号化の併用 | P.37 |
| | 対策レベル 4 | 4-1 | ● ノートパソコンやタブレット内のドライブ暗号化とファイル暗号化、並びにリモートワイプ設定の併用 | P.38 |
| | | 4-2 | ● 指紋認証機能・TPM 付き高セキュリティノートパソコン内のドライブ暗号化及びファイル暗号化の併用 | P.39 |
| | | 4-3 | ● ノートパソコン内のドライブ暗号化と鍵サーバ管理型ファイル暗号化の併用 | P.39 |
| (ii) 携帯電話・スマートフォン | 対策レベル 1 | 1-1 | ● 携帯電話・スマートフォンの利用者認証の実施 | P.41 |
| | 対策レベル 2 | 2-1 | ● スマートフォン内のドライブ暗号化の実施 | P.41 |
| | | 2-2 | ● スマートフォンや携帯電話の利用者認証の実施とファイル暗号化の併用 | P.41 |
| | 対策レベル 3 | 3-1 | ● スマートフォン内のドライブ暗号化とリモートワイプ機能設定の併用 | P.42 |
| | | 3-2 | ● スマートフォン内のドライブ暗号化とファイル暗号化の併用 | P.42 |
| | 対策レベル 4 | 4-1 | ● スマートフォン内のドライブ暗号化とファイル暗号化､並びにリモートワイプ設定の併用 | P.43 |
| (iii) USB メモリ・外付けドライブストレージ | 対策レベル 1 | 1-1 | ● USB メモリ内のセキュリティ領域設定の実施 | P.44 |
| | | 1-2 | ● ファイル暗号化の実施 | P.44 |
| | 対策レベル 2 | 2-1 | ● USB メモリ内のセキュリティ領域設定の実施 | P.44 |
| | | 2-2 | ● ファイル暗号化の実施 | P.45 |
| | 対策レベル 3 | 3-1 | ● 指紋認証付セキュリティ USB メモリの利用<br>● カード認証付外付けセキュリティドライブの利用 | P.45 |
| | | 3-2 | ● USB メモリ内のセキュリティ領域設定とファイル暗号化の併用 | P.45 |
| | 対策レベル 4 | 4-1 | ● セキュリティハードウェア内で暗号化処理を行う指紋認証付セキュリティ USB メモリの利用 | P.46 |
| | | 4-2 | ● USB メモリ内のセキュリティ領域設定、及び鍵サーバ管理型ファイル暗号化の併用 | P.46 |

### (i) ノートパソコン・タブレット

**【対策レベル 1】**

- **対策レベル 1-1：**

  例：ノートパソコンやタブレットの利用者認証の実施

  **《実施すべき項目》**

  - ■ A.1 (実践編-3) 端末ロックによる利用者認証の有効化

  **〔実施が望ましい項目〕**

  - ➢ A.2 (実践編-3) 端末ロックによる利用者認証の安全性強化
  - ➢ B.1 (実践編-4) ファイル暗号化の有効化
  - ➢ C.1 (実践編-5) ドライブ／フォルダの暗号化設定と端末ロックによる利用者認証の有効化

**【対策レベル 2】**

- **対策レベル 2-1：**

  例：ノートパソコンやタブレット内のドライブ暗号化の実施

  **《実施すべき項目》**

  - ■ A.1 (実践編-3) 端末ロックによる利用者認証の有効化
  - ■ A.2 (実践編-3) 端末ロックによる利用者認証の安全性強化
  - ■ C.1 (実践編-5) ドライブ／フォルダの暗号化設定と端末ロックによる利用者認証の有効化

  **〔実施が望ましい項目〕**

  - ➢ A.3 (実践編-3) 端末ロックによる利用者認証のさらなる安全性強化
  - ➢ C.2 (実践編-5) 端末起動時の利用者認証の有効化
  - ➢ C.3 (実践編-5) 端末起動時および端末ロックによる利用者認証の安全性強化

- **対策レベル 2-2：**

  例：ノートパソコンやタブレットの利用者認証の実施とファイル暗号化の併用

  **《実施すべき項目》**

  - ■ A.1 (実践編-3) 端末ロックによる利用者認証の有効化
  - ■ A.2 (実践編-3) 端末ロックによる利用者認証の安全性強化

■ B.1 (実践編-4) ファイル暗号化の有効化
■ B.2 (実践編-4) 暗号化ファイルに対するアクセス制御の強化

〔実施が望ましい項目〕
➢ A.3 (実践編-3) 端末ロックによる利用者認証のさらなる強化
➢ B.3 (実践編-4) 暗号化ファイルに対するアクセス制御のさらなる強化

## 【対策レベル 3】

- **対策レベル 3-1：**

例 1：指紋認証機能付き高セキュリティノートパソコン内のドライブ暗号化の実施
例 2：ノートパソコン内のドライブ暗号化と利用者認証用 USB トークンの併用
例 3：タブレット内のドライブ暗号化とリモートワイプ設定の併用

《実施すべき項目》
■ A.1 (実践編-3) 端末ロックによる利用者認証の有効化
■ A.2 (実践編-3) 端末ロックによる利用者認証の安全性強化
■ A.3 (実践編-3) 端末ロックによる利用者認証のさらなる安全性強化
■ C.1 (実践編-5) ドライブ／フォルダの暗号化設定と端末ロックによる利用者認証の有効化
■ C.2 (実践編-5) 端末起動時の利用者認証の有効化
■ C.3 (実践編-5) 端末起動時および端末ロックによる利用者認証の安全性強化

〔実施が望ましい項目〕
➢ B.1 (実践編-4) ファイル暗号化の有効化
➢ B.2 (実践編-4) 暗号化ファイルに対するアクセス制御の強化
➢ B.3 (実践編-4) 暗号化ファイルに対するアクセス制御のさらなる強化
➢ C.4 (実践編-6) 暗号化データに対するアクセス制御の強化
➢ C.5 (実践編-6) 暗号鍵の管理強化

- **対策レベル 3-2：**

例：ノートパソコンやタブレット内のドライブ暗号化とファイル暗号化の併用

《実施すべき項目》
■ A.1 (実践編-3) 端末ロックによる利用者認証の有効化
■ A.2 (実践編-3) 端末ロックによる利用者認証の安全性強化

■ A.3 (実践編-3) 端末ロックによる利用者認証のさらなる安全性強化
■ B.1 (実践編-4) ファイル暗号化の有効化
■ B.2 (実践編-4) 暗号化ファイルに対するアクセス制御の強化
■ C.1 (実践編-5) ドライブ／フォルダの暗号化設定と端末ロックによる利用者認証の有効化
■ C.2 (実践編-5) 端末起動時の利用者認証の有効化

〔実施が望ましい項目〕
➢ B.3 (実践編-4) 暗号化ファイルに対するアクセス制御のさらなる強化
➢ C.3 (実践編-5) 端末起動時および端末ロックによる利用者認証の安全性強化
➢ C.4 (実践編-6) 暗号化データに対するアクセス制御の強化
➢ C.5 (実践編-6) 暗号鍵の管理強化

## 【対策レベル 4】

- **対策レベル 4-1：**
  例：ノートパソコンやタブレット内のドライブ暗号化とファイル暗号化、並びにリモートワイプ設定の併用

《実施すべき項目》
■ A.1 (実践編-3) 端末ロックによる利用者認証の有効化
■ A.2 (実践編-3) 端末ロックによる利用者認証の安全性強化
■ A.3 (実践編-3) 端末ロックによる利用者認証のさらなる安全性強化
■ B.1 (実践編-4) ファイル暗号化の有効化
■ B.2 (実践編-4) 暗号化ファイルに対するアクセス制御の強化
■ C.1 (実践編-5) ドライブ／フォルダの暗号化設定と端末ロックによる利用者認証の有効化
■ C.2 (実践編-5) 端末起動時の利用者認証の有効化
■ C.3 (実践編-5) 端末起動時および端末ロックによる利用者認証の安全性強化
■ C.4 (実践編-6) 暗号化データに対するアクセス制御の強化

〔実施が望ましい項目〕
➢ B.3 (実践編-4) 暗号化ファイルに対するアクセス制御のさらなる強化
➢ C.5 (実践編-6) 暗号鍵の管理強化
➢ C.6 (実践編-7) セキュリティ認証製品の採用

- **対策レベル 4-2：**

  例：指紋認証機能・TPM 付き高セキュリティノートパソコン内のドライブ暗号化及びファイル暗号化の併用

  **《実施すべき項目》**

  - ■ A.1（実践編-3）端末ロックによる利用者認証の有効化
  - ■ A.2（実践編-3）端末ロックによる利用者認証の安全性強化
  - ■ A.3（実践編-3）端末ロックによる利用者認証のさらなる安全性強化
  - ■ B.1（実践編-4）ファイル暗号化の有効化
  - ■ B.2（実践編-4）暗号化ファイルに対するアクセス制御の強化
  - ■ C.1（実践編-5）ドライブ／フォルダの暗号化設定と端末ロックによる利用者認証の有効化
  - ■ C.2（実践編-5）端末起動時の利用者認証の有効化
  - ■ C.3（実践編-5）端末起動時および端末ロックによる利用者認証の安全性強化
  - ■ C.5（実践編-6）暗号鍵の管理強化

  **〔実施が望ましい項目〕**

  - ➢ B.3（実践編-4）暗号化ファイルに対するアクセス制御のさらなる強化
  - ➢ C.4（実践編-6）暗号化データに対するアクセス制御の強化
  - ➢ C.6（実践編-7）セキュリティ認証製品の採用

- **対策レベル 4-3：**

  例：ノートパソコン内のドライブ暗号化と鍵サーバ管理型ファイル暗号化の併用

  **《実施すべき項目》**

  - ■ A.1（実践編-3）端末ロックによる利用者認証の有効化
  - ■ A.2（実践編-3）端末ロックによる利用者認証の安全性強化
  - ■ A.3（実践編-3）端末ロックによる利用者認証のさらなる安全性強化
  - ■ B.1（実践編-4）ファイル暗号化の有効化
  - ■ B.2（実践編-4）暗号化ファイルに対するアクセス制御の強化
  - ■ B.3（実践編-4）暗号化ファイルに対するアクセス制御のさらなる強化
  - ■ C.1（実践編-5）ドライブ／フォルダの暗号化設定と端末ロックによる利用者認証の有効化
  - ■ C.2（実践編-5）端末起動時の利用者認証の有効化
  - ■ C.3（実践編-5）端末起動時および端末ロックによる利用者認証の安全性強化

  **〔実施が望ましい項目〕**

  - ➢ C.4（実践編-6）暗号化データに対するアクセス制御の強化

- C.5 (実践編-6) 暗号鍵の管理強化
- C.6 (実践編-7) セキュリティ認証製品の採用

### （ii） 携帯電話・スマートフォン

**【対策レベル 1】**

- **対策レベル 1-1：**

  例：携帯電話・スマートフォンの利用者認証の実施

  **《実施すべき項目》**

  - ■ A.1（実践編-3）端末ロックによる利用者認証の有効化

  **〔実施が望ましい項目〕**

  - ➢ A.2（実践編-3）端末ロックによる利用者認証の安全性強化
  - ➢ B.1（実践編-4）ファイル暗号化の有効化
  - ➢ C.1（実践編-5）ドライブ／フォルダの暗号化設定と端末ロックによる利用者認証の有効化

**【対策レベル 2】**

- **対策レベル 2-1：**

  例：スマートフォン内のドライブ暗号化の実施

  **《実施すべき項目》**

  - ■ A.1（実践編-3）端末ロックによる利用者認証の有効化
  - ■ A.2（実践編-3）端末ロックによる利用者認証の安全性強化
  - ■ C.1（実践編-5）ドライブ／フォルダの暗号化設定と端末ロックによる利用者認証の有効化

  **〔実施が望ましい項目〕**

  - ➢ A.3（実践編-3）端末ロックによる利用者認証のさらなる安全性強化
  - ➢ C.2（実践編-5）端末起動時の利用者認証の有効化
  - ➢ C.3（実践編-5）端末起動時および端末ロックによる利用者認証の安全性強化

- **対策レベル 2-2：**

  例：スマートフォンや携帯電話の利用者認証の実施とファイル暗号化の併用

  **《実施すべき項目》**

  - ■ A.1（実践編-3）端末ロックによる利用者認証の有効化
  - ■ A.2（実践編-3）端末ロックによる利用者認証の安全性強化

■ B.1 (実践編-4) ファイル暗号化の有効化
■ B.2 (実践編-4) 暗号化ファイルに対するアクセス制御の強化

〔実施が望ましい項目〕
➢ A.3 (実践編-3) 端末ロックによる利用者認証のさらなる強化
➢ B.3 (実践編-4) 暗号化ファイルに対するアクセス制御のさらなる強化

【対策レベル 3】

- **対策レベル 3-1：**
  例：スマートフォン内のドライブ暗号化とリモートワイプ機能設定の併用

  《実施すべき項目》
  ■ A.1 (実践編-3) 端末ロックによる利用者認証の有効化
  ■ A.2 (実践編-3) 端末ロックによる利用者認証の安全性強化
  ■ A.3 (実践編-3) 端末ロックによる利用者認証のさらなる安全性強化
  ■ C.1 (実践編-5) ドライブ／フォルダの暗号化設定と端末ロックによる利用者認証の有効化
  ■ C.2 (実践編-5) 端末起動時の利用者認証の有効化
  ■ C.3 (実践編-5) 端末起動時および端末ロックによる利用者認証の安全性強化

  〔実施が望ましい項目〕
  ➢ B.1 (実践編-4) ファイル暗号化の有効化
  ➢ B.2 (実践編-4) 暗号化ファイルに対するアクセス制御の強化
  ➢ B.3 (実践編-4) 暗号化ファイルに対するアクセス制御のさらなる強化
  ➢ C.4 (実践編-6) 暗号化データに対するアクセス制御の強化
  ➢ C.5 (実践編-6) 暗号鍵の管理強化

- **対策レベル 3-2：**
  例：スマートフォン内のドライブ暗号化とファイル暗号化の併用

  《実施すべき項目》
  ■ A.1 (実践編-3) 端末ロックによる利用者認証の有効化
  ■ A.2 (実践編-3) 端末ロックによる利用者認証の安全性強化
  ■ A.3 (実践編-3) 端末ロックによる利用者認証のさらなる安全性強化
  ■ B.1 (実践編-4) ファイル暗号化の有効化

- ■ B.2 (実践編-4) 暗号化ファイルに対するアクセス制御の強化
- ■ C.1 (実践編-5) ドライブ／フォルダの暗号化設定と端末ロックによる利用者認証の有効化
- ■ C.2 (実践編-5) 端末起動時の利用者認証の有効化

〔実施が望ましい項目〕

- ➢ B.3 (実践編-4) 暗号化ファイルに対するアクセス制御のさらなる強化
- ➢ C.3 (実践編-5) 端末起動時および端末ロックによる利用者認証の安全性強化
- ➢ C.4 (実践編-6) 暗号化データに対するアクセス制御の強化
- ➢ C.5 (実践編-6) 暗号鍵の管理強化

## 【対策レベル 4】

- **対策レベル 4-1：**

  例：スマートフォン内のドライブ暗号化とファイル暗号化、並びにリモートワイプ設定の併用

《実施すべき項目》

- ■ A.1 (実践編-3) 端末ロックによる利用者認証の有効化
- ■ A.2 (実践編-3) 端末ロックによる利用者認証の安全性強化
- ■ A.3 (実践編-3) 端末ロックによる利用者認証のさらなる安全性強化
- ■ B.1 (実践編-4) ファイル暗号化の有効化
- ■ B.2 (実践編-4) 暗号化ファイルに対するアクセス制御の強化
- ■ C.1 (実践編-5) ドライブ／フォルダの暗号化設定と端末ロックによる利用者認証の有効化
- ■ C.2 (実践編-5) 端末起動時の利用者認証の有効化
- ■ C.3 (実践編-5) 端末起動時および端末ロックによる利用者認証の安全性強化
- ■ C.4 (実践編-6) 暗号化データに対するアクセス制御の強化

〔実施が望ましい項目〕

- ➢ B.3 (実践編-4) 暗号化ファイルに対するアクセス制御のさらなる強化
- ➢ C.5 (実践編-6) 暗号鍵の管理強化
- ➢ C.6 (実践編-7) セキュリティ認証製品の採用

### (iii) USB メモリ・外付けドライブストレージ

**【対策レベル 1】**

- **対策レベル 1-1：**

  例：USB メモリ内のセキュリティ領域設定の実施

  **《実施すべき項目》**

  - ■ C.1 (実践編-5) ドライブ／フォルダの暗号化設定と端末ロックによる利用者認証の有効化

  **〔実施が望ましい項目〕**

  - ➢ C.2 (実践編-5) 端末起動時の利用者認証の有効化

- **対策レベル 1-2：**

  例：ファイル暗号化の実施

  **《実施すべき項目》**

  - ■ B.1 (実践編-4) ファイル暗号化の有効化

  **〔実施が望ましい項目〕**

  - ➢ B.2 (実践編-4) 暗号化ファイルに対するアクセス制御の強化

**【対策レベル 2】**

- **対策レベル 2-1：**

  例：USB メモリ内のセキュリティ領域設定の実施

  **《実施すべき項目》**

  - ■ C.1 (実践編-5) ドライブ／フォルダの暗号化設定と端末ロックによる利用者認証の有効化

  **〔実施が望ましい項目〕**

  - ➢ C.2 (実践編-5) 端末起動時の利用者認証の有効化
  - ➢ C.3 (実践編-5) 端末起動時および端末ロックによる利用者認証の安全性強化

- **対策レベル 2-2：**

  例：ファイル暗号化の実施

  **《実施すべき項目》**

  - ■ B.1（実践編-4）ファイル暗号化の有効化
  - ■ B.2（実践編-4）暗号化ファイルに対するアクセス制御の強化

  **〔実施が望ましい項目〕**

  - ➢ B.3（実践編-4）暗号化ファイルに対するアクセス制御のさらなる強化

**【対策レベル 3】**

- **対策レベル 3-1：**

  例 1：指紋認証付セキュリティ USB メモリの利用

  例 2：カード認証付外付けセキュリティドライブの利用

  **《実施すべき項目》**

  - ■ C.1（実践編-5）ドライブ／フォルダの暗号化設定と端末ロックによる利用者認証の有効化
  - ■ C.2（実践編-5）端末起動時の利用者認証の有効化
  - ■ C.3（実践編-5）端末起動時および端末ロックによる利用者認証の安全性強化

  **〔実施が望ましい項目〕**

  - ➢ B.1（実践編-4）ファイル暗号化の有効化
  - ➢ B.2（実践編-4）暗号化ファイルに対するアクセス制御の強化
  - ➢ B.3（実践編-4）暗号化ファイルに対するアクセス制御のさらなる強化
  - ➢ C.4（実践編-6）暗号化データに対するアクセス制御の強化
  - ➢ C.5（実践編-6）暗号鍵の管理強化

- **対策レベル 3-2：**

  例：USB メモリ内のセキュリティ領域設定とファイル暗号化の併用

  **《実施すべき項目》**

  - ■ B.1（実践編-4）ファイル暗号化の有効化
  - ■ B.2（実践編-4）暗号化ファイルに対するアクセス制御の強化

- C.1 (実践編-5) ドライブ／フォルダの暗号化設定と端末ロックによる利用者認証の有効化
- C.2 (実践編-5) 端末起動時の利用者認証の有効化

〔実施が望ましい項目〕

- B.3 (実践編-4) 暗号化ファイルに対するアクセス制御のさらなる強化
- C.3 (実践編-5) 端末起動時および端末ロックによる利用者認証の安全性強化
- C.4 (実践編-6) 暗号化データに対するアクセス制御の強化
- C.5 (実践編-6) 暗号鍵の管理強化

## 【対策レベル 4】

- **対策レベル 4-1：**

  例 1:セキュリティハードウェア内で暗号化処理を行う指紋認証付セキュリティ USB メモリの利用

  《実施すべき項目》

  - B.1 (実践編-4) ファイル暗号化の有効化
  - B.2 (実践編-4) 暗号化ファイルに対するアクセス制御の強化
  - C.1 (実践編-5) ドライブ／フォルダの暗号化設定と端末ロックによる利用者認証の有効化
  - C.2 (実践編-5) 端末起動時の利用者認証の有効化
  - C.3 (実践編-5) 端末起動時および端末ロックによる利用者認証の安全性強化
  - C.5 (実践編-6) 暗号鍵の管理強化

  〔実施が望ましい項目〕

  - B.3 (実践編-4) 暗号化ファイルに対するアクセス制御のさらなる強化
  - C.4 (実践編-6) 暗号化データに対するアクセス制御の強化
  - C.6 (実践編-7) セキュリティ認証製品の採用

- **対策レベル 4-2：**

  例：USB メモリ内のセキュリティ領域設定、及び鍵サーバ管理型ファイル暗号化の併用

  《実施すべき項目》

  - B.1 (実践編-4) ファイル暗号化の有効化
  - B.2 (実践編-4) 暗号化ファイルに対するアクセス制御の強化

- B.3 (実践編-4) 暗号化ファイルに対するアクセス制御のさらなる強化
- C.1 (実践編-5) ドライブ／フォルダの暗号化設定と端末ロックによる利用者認証の有効化
- C.2 (実践編-5) 端末起動時の利用者認証の有効化
- C.3 (実践編-5) 端末起動時および端末ロックによる利用者認証の安全性強化

〔実施が望ましい項目〕

- C.4 (実践編-6) 暗号化データに対するアクセス制御の強化
- C.5 (実践編-6) 暗号鍵の管理強化
- C.6 (実践編-7) セキュリティ認証製品の採用

## 【コラム⑦】リモートワイプを導入したら

暗号鍵を作るのも暗号化された情報を元の情報に戻すのも実際にはソフトウェアやハードウェアが自動的に行いますので、ランダムに生成された暗号鍵を使うことができます。ランダムに生成された暗号鍵であれば、2.4.1 節に示した電子政府推奨暗号（とりわけ AES, Camellia, KCipher-2 のいずれか）を使って暗号化された情報を解読するために必要となる計算量は $2^{128}$ 以上であり、一つ一つ暗号鍵を調べる全数探索で正しい暗号鍵を見つけ出すことは非現実的です。

つまり、2.3 節にある「何らかの不正な手段で「暗号鍵」を使うことができるようになる」ためには、暗号解読以外の方法（例えば暗号化された情報を見る権限がある利用者になりすます）で保存されている暗号鍵を利用する権限を得ることにほかなりません。こうすることによって、暗号化された情報を見ることになる、ということです。

逆に言えば、このことは、**保存されている暗号鍵を消去することができれば、（暗号化された情報を見る権限がある利用者を含めて）一切暗号化された情報を見せないようにすることができる**ということになります。

一方、最近では、様々な企業からスマートフォンやタブレットなどを中心とした端末管理サービス（MDM：Mobile Device Management）が広く提供されるようになり、その中の機能として「リモートワイプ」と呼ばれる対策が導入されているケースがあります。これは、遠隔操作によって、紛失・盗難した端末を初期化したり、内部のデータを消去したりするサービスです。

どのような手法で初期化やデータ消去を行うかは MDM サービスの提供会社によって異なると考えられますが、提供会社の中には、端末に保存しているデータを暗号化しておき、そこで使う暗号鍵を遠隔操作で消去することでリモートワイプを実現しているところもあります。

そのような仕組みのリモートワイプであれば、遠隔操作で暗号鍵を消去すると、正規の利用者であっても、金輪際、その情報を見ることができなくなりますが、情報漏えいを阻止するという点で非常に有効な手段です。同じ「リモートワイプ」という名のサービスであっても、単純に初期化コマンドを送ったり、データ消去コマンドを送信するだけの方式よりもはるかに高い安全性を提供しているといえます。

各社の MDM サービスのレベルを見極めるうえで、どのような仕組みでリモートワイプを実現しているかを参考にするのも一案です。

紛失・盗難時に**「リモートワイプによってデータを消去する」のは時間との闘い**です。

とりわけ、遠隔操作で暗号鍵を消去する方式のリモートワイプを導入したのであれば、紛失・盗難などが起きた時から時間が経過すればするほど、暗号鍵を利用する権限が不正に得られてしまう恐れが高くなります。せっかくリモートワイプで保存されている暗号鍵を消去したとしても、暗号鍵を消去する前にその暗号鍵を利用する権限が不正に得られてしまえば、情報漏えいを阻止できたかどうかはわかりません。情報のバックアップがあるなど、紛失・盗難した情報が利用できなくなっても支障がないのであれば、**迷わず暗号鍵の消去を行うべき**です。

「リモートワイプの対策を導入したのに、紛失時の罰則規定を恐れて、端末を紛失した従業員が長期間届け出を行わず、結果として暗号鍵の消去が長期間行われなかった」というのは対策導入の趣旨から見て本末転倒です。リモートワイプの対策を導入するのであれば、**端末の紛失時には速やかに届け出を行わせるルールにし、端末紛失自体の責任よりも紛失届け出遅延の責任のほうが重い**ことを明示すべきです。

著作・制作　　独立行政法人 情報処理推進機構（IPA）

編集責任

執筆者　神田 雅透　独立行政法人 情報処理推進機構
山口 利恵　独立行政法人 産業技術総合研究所
一瀬 小夜　独立行政法人 産業技術総合研究所

協力者　満塩 尚史　内閣官房 政府 CIO 室 政府 CIO 補佐官
（経済産業省 CIO 補佐官併任）
中西 悦子　総務省 総合通信基盤局電気通信事業部データ通信課 企画官
二木 真明　アルテア・セキュリティ・コンサルティング 代表
沢田 登志子　一般社団法人 EC ネットワーク 理事
松本 泰　セコム株式会社 IS 研究所
コミュニケーションプラットフォームディビジョン マネージャー
松尾 正浩　三菱総合研究所 公共ソリューション本部 主席研究員
宮内 宏　宮内宏法律事務所 弁護士

〔発 行〕
２０１３年 4月２３日　第1版



〔問い合わせ先〕

本マニュアルについてのご意見・ご要望がございましたら、下記までご連絡ください。次回改訂の際などに参考にさせていただきます。なお、個別のご質問・ご要望等にはお応えいたしかねる場合もございますので、予めご了承ください。

IPA 技術本部セキュリティセンター　暗号グループ：　isec-crypt-inq@ipa.go.jp