情報事故を起こさないための対策

インターネットサービス利用ガイドライン

2018年11月

立命館情報基盤整備委員会
クラウド環境活用整備専門部会

CONTENTS 目次

はじめに 6

第1章 情報セキュリティに関する脅威と対策 7

情報セキュリティに関する脅威 8

情報セキュリティ対策チェックリスト 10

第2章 情報事故を起こさないための対策 13

対策1 マルウェア（ウイルス） 14

1-1. セキュリティ対策ソフトを導入する 14
1-2. OS をアップデートする 16
1-3. ネットワークに接続するすべての機器をアップデートする 18
1-4. アプリケーションをアップデートする 19
1-5. 信頼できるソフトウェア以外をインストールしない 20

対策2 ID とパスワード 23

2-1. パスワードは絶対に人に教えない 23
2-2. 強力なパスワードを使う 24
2-3. パスワードの使い回しをしない 26
2-4. パスワード管理ツールにパスワードをそのまま保存しない 27
2-5. 多要素認証（多段階認証）を使う 30
2-6. ログイン履歴や変更通知メールを確認する 30

対策3 Web 32

3-1. マルウェア対策をする 33
3-2. Web ブラウザのセキュリティ機能を安易に緩めない 34
3-3. ダウンロードしたファイルは必ずスキャンする 35
3-4. Web サイトが本物かどうか確かめる 36
3-5. 詐欺を目的とした Web サイトや広告に注意する 36
3-6. 気になることがあればスキャンする 38

対策4 メール 39

4-1. 迷惑メール（スパムメール）フィルタ設定をする 40
4-2. 添付ファイル、リンクに注意する 42
4-3. 詐欺やフィッシングを疑う 44
4-4. 標的型サイバー攻撃を疑う 47
4-5. 不審なメールを見分けるポイントを理解する 50
4-6. メールの誤送信に注意する 52
4-7. 機密性の高い情報は書かない 55

対策5 通信と保存（暗号化） 56

5-1. Web サイト利用時の暗号化を確認する 57
5-2. メールは暗号化されず配信されることを意識する 59
5-3. 無線 LAN（Wi-Fi）利用時の設定を確認する 60
5-4. 機密性の高いデータを暗号化する 63

対策6 アクセス権（共有） 65

6-1. パソコンのファイル共有に注意する 66
6-2. クラウドサービスでの共有機能に注意する 67
6-3. ネットワークに接続するすべての機器の設定に注意する 71

対策7 スマートフォンなどのモバイル端末 73

7-1. 盗難・紛失時も情報にアクセスされない工夫をする 73
7-2. アプリへのアクセス許可や ID・パスワード提供に注意する 75

対策8 個人情報と権利侵害 77

8-1. パソコンやスマートフォンで収集される情報を確認する 78
8-2. Web サイト閲覧履歴などの共有範囲を確認する 78
8-3. SNS での個人情報公開に注意する 79
8-4. 知的財産や個人情報などの権利や法令を意識する 82

対策9 サービス利用 86

9-1. 信頼できるサービスを選ぶ 87
9-2. 個人情報の取扱いについて確認する 88
9-3. 預けたデータの取扱いについて確認する 89
9-4. データの保管場所、準拠法、管轄裁判所を確認する 90
9-5. データ消失に備える 91
9-6. サービスの内容変更や終了に備える 91

対策10 その他 93

10-1. 廃棄・譲渡時にデータを消去する 93
10-2. ファイル共有ソフトを使わない 96

第3章 情報事故が起きてしまったら 98

情報事故が起きたときの緊急連絡受付窓口 99

情報事故の種類別の対応事例 100

マルウェアに感染した場合の対応 100

ID・パスワードを窃取された場合の対応 101

モバイル端末や外部メディアの紛失、情報の誤送信・誤公開をした場合の対応 102

情報システムを運用管理されている方へ（ガイドライン） 103

付録 A 関連規程 104

情報セキュリティ関連の規程・ガイドライン 104

リスクマネジメント基本要項 104

学校法人立命館個人情報保護規程 104

参考資料 105

Tips、解説、事例、Column

Tips 1 Windows はセキュリティ対策ソフトを標準装備 15
Tips 2 OS のアップデートの種類とリスク 17
Tips 3 それでも感染することを認識する 21
Tips 4 キーロガー 21
Tips 5 ソーシャルエンジニアリング 24
Tips 6 パスワードの自動入力機能に注意する 28
Tips 7 ID 連携トラストフレームワークにご用心 29
Tips 8 迷惑メール（スパムメール）を報告する 41
Tips 9 架空請求からの裁判所出廷命令 52
Tips 10 秘密の質問と SNS 82
解説 1 macOS、Linux、iOS はセキュリティ対策ソフト不要？ 16
解説 2 サポートが終了した OS を使っていいのか？ 18
解説 3 ランサムウェア 22
解説 4 ブルートフォース攻撃と辞書攻撃 25
解説 5 アカウントリスト攻撃 26
解説 6 エクスプロイトツール（キット）の脅威 34
解説 7 グリーンバー 36
解説 8 アイコン偽装 43
解説 9 無線 LAN（Wi-Fi）のセキュリティキー 61
解説 10 VPN とは 61
解説 11 URL 公開機能 69
解説 12 位置情報取得機能や画像に埋め込まれる位置情報 81
解説 13 国境を越えてはいけない情報 85
事例 1 ネットワーク機器の設定ミスや脆弱性による被害 19
事例 2 Google グループの初期設定問題による情報漏えい 66
事例 3 オンラインストレージの危険性 68

事例 4 ネットワークストレージによる情報漏えい事故 71
事例 5 情報漏えい事故における盗難・紛失の割合 74
Column 1 転送や差出人変更は控えましょう 53
Column 2 無線 LAN（Wi-Fi）同士の干渉 62
Column 3 ファイル転送サービスの選び方 70
Column 4 大学・附属校が提供していないサービスやアプリ 76

付録 A 関連規程 104
参考資料 105
索引 106

はじめに

近年インターネットは社会基盤としてその地位を確立し、情報検索、ネットショッピング、予約サービス、オンラインバンクのように日常生活に浸透してきました。教育機関においても、教育・研究・管理運営になくてはならないものになりました。スマートフォンやアプリの普及により、多くの利用者はインターネットを利用しているということを意識せずその利便性を享受しています。

一方で、利用者の増加に合わせて、インターネットをはじめとした情報通信技術（ICT）を悪用して経済活動、社会生活を脅かす事例も急増し、情報漏えい、詐欺、遠隔操作、身代金要求など、様々な情報セキュリティに関する事故（情報事故）や犯罪にも発展しています。

こうした脅威に対抗するためにはサーバーシステムやネットワークシステム等を管理する情報部門だけではなく、**利用者自らが、自身の安全を守るために情報セキュリティ対策に真剣に取り組まなければなりません。生活安全のための防犯対策、交通安全対策などと同様に、情報セキュリティに関するリスクを知り、その対策を実践することが重要です。**

本書では、「情報セキュリティとはなにか」という観点ではなく、情報の漏えいや滅失、詐欺被害などの情報事故を起こさない、情報事故に遭わないために、常に心がけるべき具体的対策を中心に解説しています。

冒頭から通読していただいても、興味のある対策から読み進めていただいてかまいませんが、**まずは第 1 章「情報セキュリティに関する脅威と対策」の対策チェックリストを使って、あなたがどのくらい情報セキュリティ対策を心がけているか確認されることをお奨めします。**

本書が皆さんの情報セキュリティ対策の手助けになれば幸いです。

Chapter 1

第１章

情報セキュリティに関する脅威と対策

情報セキュリティに関する脅威

インターネットをはじめとしたICTサービスが生活に浸透したことにより、利用者自身が情報事故を起こしてしまうケース、サイバー攻撃により情報事故に遭ってしまうケースなど、その発生件数が増加し、及ぼす影響も拡大しています。情報事故を起こしたり被害に遭えば、自分のみならず他者の個人情報やプライバシーに関する情報を漏えいさせたり、意図せず犯罪に加担してしまうなど、社会的責任を問われるようなことになりかねません。

車を運転することが大きな利便性を生む反面、交通事故と無縁ではいられないように、インターネットをはじめとしたICTの利用もまた情報事故と無縁ではないことを意識せねばなりません。

では、どのように対策すればよいのでしょうか。それは防犯や交通安全と同じです。**あなたの周りに潜む情報セキュリティに関する「リスク」、すなわち、まだ起こっていないが、発生すれば影響を与える事象や状態について、できるだけ多く知り、その正しい対処方法を身につけ、実践することこそが、情報セキュリティ対策です。**

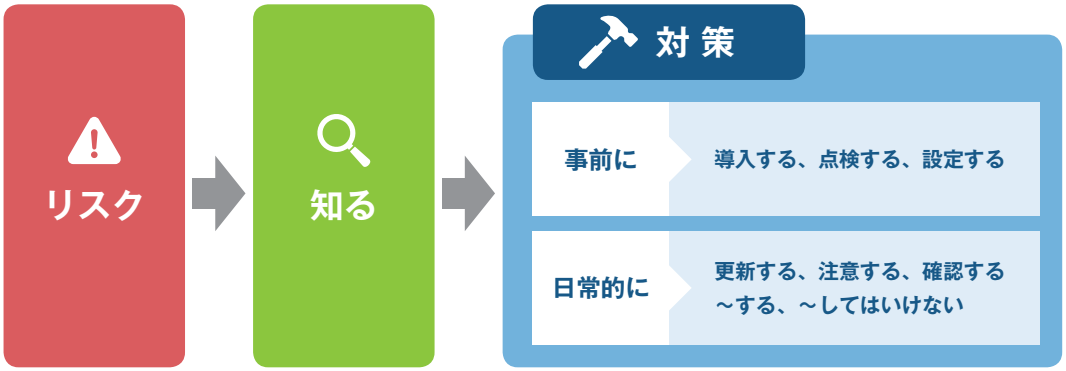


図１　情報セキュリティ対策のイメージ

情報事故は様々な要因で発生し、その対策も様々です。次章ではリスクと対策を10の分野に分け、それぞれのポイントを解説します。

情報セキュリティに関する攻撃の大半は、パソコンやスマートフォンなどのコンピューターが、マルウェア（ウイルス）という不正なプログラムに感染させられることや、ID とパスワードを窃取されることから始まります。これを端緒としてオンラインバンクやクレジットカードを不正利用される、機密性の高い情報を盗まれる、遠隔操作される、大切なデータがロックされ身代金を要求されるといった直接的な被害が発生します。対策１～２では、「マルウェア（ウイルス）に感染しないための対策」と「ID とパスワードを窃取されないための対策」について解説します。

インターネットで最も広く利用されているサービスである Web とメールは、コンピューターをマルウェア（ウイルス）に感染させる、ID とパスワードを窃取するための手段として利用されます。対策３～４では、「Web サイトやメールの信頼性を見極めるための対策」について解説します。

パソコン以外にも持ち歩く情報機器が豊富になったことにより、盗難・紛失・盗聴・設定の誤りが起きる可能性が高まり、意図せず個人や組織の情報が漏えいする情報事故が発生しています。対策５～７では、こういった事態を招かないための「アクセス権の管理」「スマートフォンなどモバイル端末の管理」、また盗難・紛失・盗聴などがあっても情報が漏えいしないための「暗号化」について解説します。

インターネットのサービスを利用する場合、他者に自分の個人情報やデータを預けていることを忘れがちです。対策８～９では、「個人情報やデータをサービス提供者に預ける場合に気をつけること」について解説します。

対策 10 では上記以外の「その他」のポイントについて解説します。

情報セキュリティ対策チェックリスト

以下のチェックリストを使って、どれくらい情報セキュリティを意識しているかを確認しましょう。情報セキュリティ対策チェック項目を**満たしている場合、もしくは、そのサービスや機器を利用していない場合はチェックをつけてください**。

チェックをつけなかった項目（設問や単語の意味が分からない場合も含む）については、第２章「情報事故を起こさないための対策」で解説する各対策ポイントをよく読んで理解しましょう。

■ 情報セキュリティ対策チェック項目 ■

対策１	マルウェア（ウイルス）	
1-1	パソコン、スマートフォンなどの機器には、セキュリティ対策ソフトを導入し利用している	☐
1-2	パソコン、スマートフォンなどの OS は定期的にアップデートしている	☐
1-3	ネットワークに接続する機器は定期的にファームウェアをアップデートしている	☐
1-4	OS 以外のアプリケーション（スマートフォンのアプリを含む）も定期的にアップデートしている	☐
1-5	ソフトウェアをインストールする前に、メーカーや提供者、配布元の信頼性を確認している	☐

対策2	ID とパスワードの管理	
2-1	自分が使用しているパスワードは、システム管理者にも絶対に教えない	☐
2-2	パスワードの強度について理解し、強力なパスワードを使用している	☐
2-3	複数のサービスで同じパスワードを使用（使いまわし）していない	☐
2-4	パスワード管理ツールを使って ID とパスワードを管理しており、管理ツールにパスワード文字列そのものを入力していない	☐
2-5	多要素認証を積極的に使っている、また機密性の高いデータを預ける場合は多要素認証のあるサービスを選んでいる	☐
2-6	ログイン履歴を定期的に確認している	☐

対策3　Web サイト

3-1	危険な Web サイトを判別し、警告を通知するセキュリティ対策ソフトを使っている	☐
3-2	Web ブラウザのセキュリティ設定を必要以上に緩めていない	☐
3-3	Web サイトからダウンロードしたファイルは、必ずマルウェアスキャンしてから使用している	☐
3-4	偽の Web サイトに誘導されていないか気をつけている	☐
3-5	詐欺を目的とした Web サイトや広告の見分けがつく	☐
3-6	怪しい Web サイトを閲覧した場合や身に覚えのない警告が出た場合、セキュリティ対策ソフトで機器をフルスキャンするようにしている	☐

対策4　メール

4-1	迷惑メールフィルタを活用しており、定期的に迷惑メールフォルダに仕分けられたメールも確認している	☐
4-2	メールの添付ファイルや本文内のリンクを開く場合は、細心の注意を払っている	☐
4-3	心当たりのない受信メールは詐欺メールかもしれないと常に疑っている	☐
4-3	フィッシングメールについて理解しており、見分けることができる	☐
4-4	標的型攻撃メールについて理解しており、見分けることができる	☐
4-5	不審なメールを見分けるポイントを把握している	☐
4-6	メールの誤送信をしないよう常に注意している	☐
4-7	機密性の高い情報をメールに書かないように（または添付しないように）気をつけている	☐

対策5　暗号化

5-1	Web サイト利用時に通信が暗号化されているか否か見分けがつく	☐
5-2	メールは盗聴される可能性があることを知っている	☐
5-3	無線 LAN（Wi-Fi）接続の暗号方式と、自宅・職場以外で接続する場合の危険性を理解している	☐
5-3	無線 LAN ルーター（Wi-Fi ルーター）のセキュリティ機能を理解しており、適切な設定をおこなっている	☐
5-4	パソコン、スマートフォン、USB メモリ、SD カードなどのデータを暗号化する方法を知っており、必要に応じて使用している	☐

対策6　アクセス権の管理

6-1	パソコンのファイル共有設定を行う場合、共有する相手は必ず最小限にしている	☐
6-2	オンラインストレージを利用する場合は、機密性のあるデータをインターネットに公開しないよう設定に注意している	☐
6-3	ネットワークに接続する機器には、適切なセキュリティ設定をしている	☐

対策7　スマートフォンなどモバイル端末の管理

7-1	スマートフォンなどモバイル端末を紛失したり盗難に遭っても、他人に使用されたりデータを取り出されたりしないための設定をしている	☐
7-2	スマートフォンやタブレットのアプリがアクセスする機能（カメラや位置情報、連絡先など）やデータについて確認している	☐

対策8　個人情報と権利侵害

8-1	パソコンやスマートフォン経由で利用者情報が収集される場合があることを理解し、適切な制限設定をしている	☐
8-2	自分以外も利用するパソコンを使う場合は、Web サイトの閲覧履歴がどのように記録され、他の利用者にどのように共有されるか理解している	☐
8-3	SNS では、情報の組合せや写真の位置情報などで個人が特定される場合があることを理解し、公開範囲の設定などにも配慮している	☐
8-4	「知的財産権」「個人情報保護」やデータ移動に関する法令（外為法、GDPR）について、基礎的なことを理解している	☐

対策9　サービス提供者との取り決めを確認する

9-1	インターネット上のサービスを使う場合は、提供者やサービスが信頼できるか否か確認している	☐
9-2	インターネットのサービスに個人情報を入力する場合は、そのサービスの個人情報の取り扱いポリシーを確認している	☐
9-3	メールやオンラインストレージなどデータを預けるサービスを利用する場合は、サービス利用規約等で提供者側のデータ利用範囲を確認している	☐
9-4	インターネット上のサービスを使う場合は、データがどこに保管され、係争時に適用される法令について確認している	☐
9-5	メールやオンラインストレージなどデータを預けるサービスを利用する場合は、システム障害などによるデータ消失に備え、データのバックアップをしている	☐
9-6	インターネット上のサービスを利用するときは、提供者の都合で変更されることを意識して、常に備えている	☐

対策10　その他

10-1	パソコン、スマートフォン、ネットワークストレージ（NAS）など、機密性の高い情報を格納した機器は、廃棄・譲渡時にデータを完全に消去したり、物理的に破壊している	☐
10-2	ファイル共有ソフトを利用する危険性を理解しており、利用していない	☐

Chapter 2

第2章

情報事故を起こさないための対策

対策 1

マルウェア（ウイルス）

「コンピューターウイルス」という言葉は、ほとんどの方がご存知だと思います。従来、他のファイルやプログラムに寄生して悪さをする様が生物的なウイルスに似ていることからそう呼ばれました。現在では、「スパイウェア」「ボット」「ランサムウェア」などこれまでのコンピューターウイルスの定義に当てはまらない悪意のあるソフトウェアが増加したため、悪意のある（malicious）ソフトウェアを総称して「マルウェア」と呼ぶようになりました。

マルウェアに感染すると、情報窃取、オンラインバンク不正送金、クレジットカード盗用、遠隔操作、身代金要求などあらゆる犯罪行為の下地になるため、攻撃者は第一目標として「マルウェアに感染させる」ことを目的とします。よって、ここではマルウェアに感染しないための対策を解説します。

マルウェアに関する５つのポイント

- 1-1 セキュリティ対策ソフトを導入する
- 1-2 OSをアップデートする
- 1-3 ネットワークに接続するすべての機器をアップデートする
- 1-4 アプリケーションをアップデートする
- 1-5 信頼できるソフトウェア以外をインストールしない

1-1 セキュリティ対策ソフトを導入する

簡単でかつ効果が期待できるマルウェア対策は、利用するパソコン、スマートフォンにセキュリティ対策ソフト（ウイルス対策ソフト、ワクチンソフト、アンチウイルスソフトなど様々な呼び方があります）を導入することです。セキュリティ対策ソフトは定義ファイルや

検知エンジンが自動更新されるよう設定し、**常に最新状態で使う**ようにしましょう。

しかし、セキュリティ対策ソフトを導入したから安心というわけではありません。セキュリティ対策ソフトの基本機能は「既知のマルウェア」からパソコンやスマートフォンを守ることです。マルウェアは、複数のセキュリティ対策ソフトで検知されないことを確認してから、売られたり、サイバー攻撃に利用されたりします。「未知のマルウェア」は毎日多数発見されており、常に感染の危険性があるということです。感染した時点で検知できなかったマルウェアも、定期的なスキャンにより発見できることがあります。セキュリティ対策ソフトを導入した際には**定期スキャンの設定をしておきましょう。**

近年のセキュリティ対策ソフトには「既知のマルウェア」を検知する機能に加え、「不正プログラムの動きを検知する（振る舞い検知、ヒューリスティック検知）」「ネットワーク攻撃を防ぐ（パーソナルファイアウォールや IPS/IDS）」「安全な領域ソフトウェアをテスト実行し、その動作から不正な動きを検知する（サンドボックス）」など様々な機能がついたものが登場しています。ソフトウェアメーカーによって呼び名がそれぞれ違いますが**「不正プログラムの動きを検知する（振る舞い検知、ヒューリスティック検知）」機能がついているものが望ましい**でしょう。これにより「未知のマルウェア」による攻撃を防げる可能性が高まります。

また、**スマートフォンにおいてもマルウェア被害が多数報告されていることから、セキュリティ対策ソフトをインストールしましょう。**

Tips 1

Windows ではセキュリティ対策ソフトを標準装備

Windows 8.1 以降では Windows Defender という機能で、セキュリティ対策ソフトが装備され、初期設定で有効になっています。これにより「セキュリティ対策ソフトを導入する」ことは最低限クリアしていることになります。現在の設定を確認し、推奨設定を変更しないようにしましょう。

解説❶

macOS、Linux、iOS はセキュリティ対策ソフト不要？

macOS、Linux、iOS などでセキュリティ対策ソフトが不要という意見があります。これらの OS もマルウェア被害の報告がされているにも関わらず、不要と誤解する要因として、1 つ目に Windows や Android と比べて、対策 1-5「信頼できるソフトウェア以外をインストールしない」が徹底されていることが多いこと、2 つ目に利益重視のサイバー攻撃において利用者の多い OS ほど狙われやすいことです。よって、「他の対策や市場シェアによって被害件数が相対的に少ない＝セキュリティ対策ソフトが不要」ということではありません。

また、セキュリティ対策ソフトは、既知のマルウェアの検知だけでなく、複数のセキュリティ対策機能があるので導入することを推奨します。（対策 3「Web」、対策 4「メール」、対策 7「スマートフォンなどのモバイル端末」参照）

1-2 OSをアップデートする

ソフトウェアから「機能の不具合やセキュリティの不具合」（以下、脆弱性）を完全に取り除くことは困難です。マルウェアの多くはこの脆弱性を衝いて、パソコンに感染します。ほとんどのコンピューターは、機器を動かすために Windows、macOS、Linux などの OS と呼ばれるソフトウェアを搭載しており、攻撃者にとっては、多くの人が使う OS は魅力ある攻撃対象です。日々新たに発見される脆弱性に対し、メーカーは OS の修正プログラムを提供しており、利用者は OS をアップデート（更新）したり、修正プログラムを適用したりすることで脆弱性を解消しマルウェアの感染リスクを低減できます。**パソコンでは Windows Update や Mac App Store のアップデート設定を確認し、セキュリティに関するアップデートは自動で適用されるように設定しましょう。**

最近では、スマートフォンを狙ったマルウェアによる被害も拡大しています。不審なアプリのインストール以外にも、メールに記載された Web サイトを閲覧しただけでマルウェアに感染する事例も Android、iOS ともに報告されています。スマートフォンもコンピューターのうちの 1 つであり、脆弱性が発見されるため、スマートフォンに使われる iOS や Android などの OS もアップデートする必要があります。**iOS や Android でも、重要なデータをバックアップした上でアップデートするようにしましょう。**

参考：ルックアウト「モバイルセキュリティアラート：iOS を標的にした高度なモバイル攻撃が発生」
https://blog.lookout.com/jp/2016/08/29/securityalertpegasus/

各 OS のアップデート確認方法

■ **Windows 10**
［設定］› ［更新とセキュリティ］› ［Windows Update］

■ **macOS**
［App Store］› ［アップデート］

■ **iOS**
［設定］› ［一般］› ［ソフトウェアアップデート］

■ **Android**
［設定］› ［端末情報］› ［ソフトウェア更新］

また、**前述のセキュリティ対策ソフトの導入と OS のアップデートは、どちらが欠けてもいけません。**例えるならセキュリティ対策ソフトは警備会社による監視、OS のアップデート（脆弱性対策）は建物の欠陥を修繕するようなものです。建物の鍵や窓などに欠陥があれば、いくら警備会社が監視をしても守り切れません。

Tips❷

OS のアップデートの種類とリスク

ソフトウェアのアップデートは大きく分けて、①機能追加・変更、②機能不具合修正、③セキュリティ対策の 3 種類です。アップデートはバージョンで示されることが多く、数字の意味合いはメーカーによってもソフトウェアによっても異なります。

例えば iOS のバージョンは 9.3.5 から 10.0、10.0.1、10.0.2、10.0.3、10.1、10.1.1、10. 2、10.2.1、10.3 と続いています。

9.3.5 の場合

左の数字：9
根本的または大幅な機能追加・変更が行われた場合に数字が増えます。
大きく機能が変わるアップデートをメジャーバージョンアップと呼びます。

真ん中の数字：3
一部機能の追加・変更、脆弱性対策など、主たる機能を変更しないアップデートをマイナーバージョンアップと呼びます。

右の数字：5
脆弱性対策など、機能の追加変更をしないアップデートをマイナーバージョンアップまたはバグ修正やバグフィックスなどと呼びます。

マルウェア対策としてソフトウェアのアップデートを行うことは重要ですが、一方アップデートを行うことで、使い勝手が変わる、必要な機能が廃止される、新たな不具合が生じる、アップデート自体が失敗するといった問題が起こることもあります。こういった場合に備え、安定稼働を必要とするシステムのアップデータや、他のソフトウェアの動作に影響を与える OS のメジャーバージョンアップを行う前には重要なデータや設定情報をバックアップしたり、新バージョンの評判などを調べることをお奨めします。

解説❷

サポートが終了した OS を使っていいのか？

2014 年に Microsoft 社が Windows XP のサポートを終了したことは、新聞やニュースなどで報じられ話題となりました。サポート終了後は、脆弱性が発見されても修正プログラムが配布されることはありません。また、次々と高度化・巧妙化するサイバー攻撃に対して、新しいセキュリティ対策が追加されることもありません。いわば解錠方法が広く知られた錠しかない金庫に重要な情報を保管しているようなものです。たとえサポートが終了した OS に現在も対応しているセキュリティ対策ソフトがあっても、先に述べた通りサポートが終了した OS の脆弱性そのものが解消されない状態を安全だと誤解してはいけません。

サポートが終了した OS を使い続けることは、自分自身への被害の発生はもちろん、加害者になり得る可能性もあり、絶対に避けるべきです。

1-3 ネットワークに接続するすべての機器をアップデートする

脆弱性対策をしなければならない機器は、パソコン、スマートフォンだけではありません。近年、プリンタ、複合機、ブロードバンドルーター（無線 LAN アクセスポイント含む）、ネットワークストレージ（NAS）、ネットワークカメラ（監視カメラ、Web カメラ）などのネットワーク機器だけでなく、テレビ、HDD レコーダー、家庭用ゲーム機などのデジタル家電がインターネットに接続されるようになりました。

これらの機器もそれぞれ OS にあたるファームウェアと呼ばれる組込みソフトウェアにより動いており、インターネットに接続することで、脆弱性を狙った攻撃を受ける危険性にさ

らされています。

ネットワークに接続する機器を購入・設置した際は、マニュアルをよく読み**ファームウェアの自動更新設定があればオンにしましょう。また、自動更新設定がなければ、定期的にメーカーのサイトを確認しファームウェアの更新（脆弱性対策）をしましょう。**

事例❶

ネットワーク機器の設定ミスや脆弱性による被害

2014 年頃から、監視カメラやネットワークカメラ（Web カメラ含む）の脆弱性を悪用しカメラの映像を不正アクセスにより窃取する事件が増えています。2016 年 1 月には、世界中の監視カメラから窃取した映像を公開する Web サイトが発見され新聞やニュースで大きな話題となりました。

また、2016 年 5 月にはトレンドマイクロ社が、ネットワークに接続されたテレビの脆弱性を衝いて、使用不可にするランサムウェアの存在を報告しています。

1-4 アプリケーションをアップデートする

OS 上で動作する特定作業の目的に応じて使うソフトウェアのことをアプリケーションソフトウェアと言い、Web ブラウザ・ワープロ・表計算などのソフトウェアがこれにあたります。また、スマートフォンでは、省略して「アプリ」と呼ぶことが一般的になりました。マルウェアはこうしたアプリケーションの脆弱性を衝くものも非常に多く、特に Web ブラウザ（Internet Explorer，Google Chrome など）、Adobe Flash Player、Adobe Reader、Java（Java Runtime Environment）、Microsoft Office などよく使われるアプリケーションへの攻撃が多数報告されています。対策 3「Web」、対策 4「メール」で後述しますが、アプリケーションの脆弱性対策をすることでマルウェア感染のリスクは大きく低減できます。**Web ブラウザに代表されるような多くの人が利用するアプリケーションは特にマルウェアの攻撃対象となりやすいため、可能な限り自動更新するようにしましょう。**

iOS や Android で使用しているアプリも定期的にアップデートし、最新の状態に保つようにしましょう。

1-5 信頼できるソフトウェア以外をインストールしない

パソコンやスマートフォンに信頼できないソフトウェアを安易にインストールすることはやめましょう。メーカー（制作者）の身元がはっきりしている、または利用者からの評価が高いソフトウェアを選び、かつ必要なものだけをインストールするようにしましょう。

信頼できるソフトウェア入手先

■ **パソコン**
Windows ストア、Mac App Store、量販店での商用パッケージ、フリーウェアやシェアウェアは窓の杜や Vector など

■ **スマートフォン・タブレット**
App Store、GooglePlay

ソフトウェアの入手先は信頼できるところに限定し、メーカー（制作者）、利用者評価なども確認しましょう。

スマートフォンを狙ったマルウェアの多くは、マルウェアであることを隠し利用者にインストールを促します。「バッテリーが長持ち」「無償のセキュリティ対策ソフト」といった広告などに誘われ、インストールするケースがパソコンより多くなっています。

また、**提供元不明のアプリをインストールできなくしている初期設定を変更したり、改造（いわゆる Root 化や脱獄）したりするのは危険ですのでやめましょう。**

参考：G DATA　Software AG　G DATA による 2015 年マルウェア動向予測
http://gshop.g-wise.co.jp/blog/presscenter/マルチターゲット型スパイウェアにより企業情報.html

参考：スマートフォンがマルウェア感染した場合の 5 つの兆候
https://eset-info.canon-its.jp/malware_info/special/detail/160216.html

参考：KASPERSKY　Root 化と脱獄のメリット、デメリット
https://blog.kaspersky.co.jp/rooting-and-jailbreaking/892/

Tips 3

それでも感染することを認識する

新しい脆弱性が発見されたり、新たな攻撃手法が出現してからメーカーなどによる対策が講じられるまでの間になされる攻撃は「ゼロデイ攻撃（0 day Attack）」と呼ばれ、この攻撃を利用者自身が防ぐことは非常に困難です。

重大な脆弱性や新種の手口による脅威の情報は、インターネット上のニュースや登録しているサービスからの注意喚起メール、セキュリティ情報を発信するサイトなどで得られます。これらの情報を定期的に確認し、迅速に対応しましょう。

参考：IPA（情報推進化機構）情報セキュリティ
http://www.ipa.go.jp/security/personal/index.html

Tips 4

キーロガー

キーボードからの入力を記録（logging）するソフトウェアもしくはハードウェアをキーロガーと呼びます。すべてのキーロガーがマルウェアというわけではなく、データバックアップ、監視や証跡管理、ペアレンタルコントロールなどで有用に使われています。一方、情報の窃取を目的とした悪意あるキーロガーもインターネット上には存在します。悪意あるキーロガーが組み込まれたパソコンではキーボードで入力した ID やパスワード、クレジットカード番号などが窃取され犯罪に利用されるケースがあります。また、クリップボードも対象にするキーロガー、パソコンとキーボードの間に接続する USB 機器型キーロガーなどもあります。

オンラインバンクや EC サイトなどでキーロガー対策としてソフトウェアキーボードが用意されている場合があります。なるべく使うようにしましょう。

参考：トレンドマイクロ is702「ネットバンクの預金残高が 0 に！新手のデジタル空き巣」
https://www.is702.jp/column/402/

解説❸

ランサムウェア

マルウェアの一種で、身代金（ransom）を要求することからランサムウェアと呼びます。ランサムウェアに感染するとパソコンがロックされたり、パソコン上やネットワーク上のファイルがロックされます。ロックされたパソコンやファイルを開こうとするとロック解除のための身代金を要求されます。

要求に応じてもデータが戻らない事例も多く、犯罪者に資金を与えることで、新たなマルウェアや犯罪を生むことにつながるため、決して身代金を支払ってはいけません。**マルウェア感染に備え普段から重要なデータのバックアップをおこないましょう。**

参考：トレンドマイクロ「ランサムウェアとは？」
http://www.trendmicro.co.jp/jp/security-intelligence/threat-solution/ransomware/index.html

対策 2

ID とパスワード

様々なサービスで ID とパスワードの組合せによる本人確認をしています。ID とパスワードによる認証はクレジットカードや銀行口座の暗証番号と同様に「本人しかパスワードを知らない」という前提で運用しており、ID とパスワードが攻撃者に知られてしまうと、あなたの情報や金銭が窃取される、あなたになりすました攻撃者が第三者に危害を加えるといった事態につながります。そのような事態を招かないためには ID とパスワードを正しく管理することが大切です。

ここでは ID とパスワードがどのように漏えいするのかを紹介し、その対策を解説します。

ID とパスワードに関する 6 つのポイント

2-1 パスワードは絶対に人に教えない

2-2 強力なパスワードを使う

2-3 パスワードの使い回しをしない

2-4 パスワード管理ツールにパスワードをそのまま保存しない

2-5 多要素認証（多段階認証）を使う

2-6 ログイン履歴や変更通知メールを確認する

2-1 パスワードは絶対に人に教えない

サービスを利用するためのパスワードはあなただけが知るべき情報です。例え**システム管理者であっても、あなたにパスワードを聞くことはありません。もしパスワードを聞かれたら、まず詐欺を疑ってください。**

Tips 5

ソーシャルエンジニアリング

ソーシャルエンジニアリングとは、ICT の仕組みを使わずに ID やパスワードを窃取する手口です。巧みにあなたの心理的な隙や行動のミスにつけこんでパスワードを盗み取ろうとしてきます。このような手口に対しても十分に注意してください。

＜ソーシャルエンジニアリングの例＞

- 電話でシステム管理者を装ってパスワードを聞く
- キー入力を盗み見る（ショルダーハッキング）
- ゴミ箱をあさる（トラッシング）
- 建物に侵入する

参考：総務省　国民のための情報セキュリティサイト　「ソーシャルエンジニアリングの対策」
http://www.soumu.go.jp/main_sosiki/joho_tsusin/security/business/staff/12.html

2-2 強力なパスワードを使う

パスワードには「強度」という考え方があります。「強度が高い」＝「推測しにくい」ということです。例えば、数字４桁のパスワードがあったとします。状況にもよりますが、コンピューター（計算機）の世界では数秒で解析されてしまう恐れがあります。

パスワードを設定する際のポイント

- 覚えやすい
- 辞書にある単語や固有名詞を使わない
- 文字数は８文字以上にする（12 文字程度を推奨）
- 文字の種類は大文字、小文字、数字、記号を組合せる
- 変換ルールやアナグラムを使う

あなたもしくは家族の名前や個人情報に関連する数字（生年月日、電話番号、記念日など）をパスワードに使うことは大変危険です。特に自身や身近な人の SNS から推測されるケースも増えていますので、個人情報を安易にパスワードに使うのはやめましょう。

名前や辞書にある言葉を使う場合は、一部を数字や記号にすることで推測は難しくなりま

す。パスワードの強度チェッカーや強力なパスワードを作成するコツなどを紹介する Web サイトなどを参考に強力なパスワードを作成しましょう。

強力なパスワードの作成例

①好きな英文を考える

Don’t put all your eggs in one basket.

②オリジナルのルールに基づいて文章をつなげる

Dpayeiob　←頭文字をつなげています

③オリジナルの変換ルールで文字を置き換える

Dp@yE!06 ←「a」「i」「o」「b」を似た記号や数字に変換

辞書にある単語を元に③のみを行ってパスワードを作成することはお勧めできません。「Password」→「P@$$w0rd」のような文字変換は攻撃者が容易に想定できるためです。

参考：トレンドマイクロ「パスワード」
https://www.is702.jp/column/542/

過去には定期的なパスワードの変更を推奨されたこともあります。しかし現在ではその必要はなく、それぞれのサービスで個別の強力なパスワードを使うべきとされています。その理由として、定期的なパスワードの変更は、パスワードを覚えることが優先され、ワンパターン化や単純化、使い回しなどにより、容易に推測されるようになるためです。

解説❹

ブルートフォース攻撃と辞書攻撃

パスワードの強度が低いと、ブルートフォース攻撃（総当たり攻撃）や辞書攻撃と呼ばれる攻撃によりパスワードを窃取されます。これらはその名の通り、片っ端から単語や文字の組合せを試す攻撃で、強度の低いパスワードには非常に脅威となる攻撃です。

2-3 パスワードの使い回しをしない

あなたのパスワード管理が完璧であったとしても、利用するサービスが脆弱性を抱えており、ID やパスワードが窃取され流出するケースがあります。そのような場合、他のサービスで同じパスワードを使っていたらどうなるでしょうか。ID やパスワードが流出したサービスだけでなく、あなたが使っている他のサービスでも同じ ID と同じパスワードを使って不正にログインをされる可能性が高まります。このような**２次被害に遭わないよう、パスワードの使い回しをしてはいけません。**

解説❺

アカウントリスト攻撃

アカウントリスト攻撃（パスワードリスト攻撃、リスト型アカウントハッキング、リスト型攻撃などとも呼びます）とは、不正アクセスなどにより集めた ID とパスワードの組合せを様々なサービスで試す攻撃です。パスワードの使い回しをしている人ほど、被害が大きくなります。2014 年には、LINE のアカウントを乗っ取り、LINE で友達に「自分の代わりにプリペイドカードを購入してほしい」と連絡し、入手したプリペイドカードを換金するという事件が発生し大きく報道されました。この乗っ取りはアカウントリスト攻撃によるものと言われています。

また、同じパスワードにサービス名をつけ加えるようなパスワード設定もやめましょう。例えば、Google のパスワードを「pass-google」としている人がパスワードを攻撃者に窃取されたとします。Facebook のパスワードを「pass-fb」「pass-Facebook」としてアカウントリスト型攻撃やパスワードリスト攻撃を受けることになります。

Trend Micro　アカウントリスト攻撃
http://www.trendmicro.co.jp/jp/security-intelligence/threat-solution/access/index.html

2-4 パスワード管理ツールにパスワードをそのまま保存しない

インターネット上のいろいろなサービスを利用すればするほど、多数のアカウントやパスワードの管理をおこなう必要が生じます。これらの ID やパスワードはどのように管理すればよいでしょうか。ノートに書く、Word や Excel のような暗号化（パスワードロック）可能なドキュメントとして保管する、パソコンのパスワード管理ツール（機器内にのみ格納されるもの）に記録する、スマートフォンアプリのパスワード管理ツール（機器内にのみ格納されるもの）に記録するといった管理方法を取ることが一般的です。最近では、クラウドサービスを使い、あらゆるログインの局面で共通利用が可能なパスワード管理サービスも登場しています。

これらのパスワード管理の利点・欠点と使う際のポイントは以下の通りです。

パスワード管理の例とポイント

ノートに書く

○ インターネットからの攻撃や脆弱性の影響を受けない

POINT
- 紛失に備え、定期的にコピーする
- 紛失の危険性があるため、持ち歩かない
- サービスと ID とパスワードの関連性をわかりにくく記載する
- 鍵のかかる場所に保管する　●閲覧時は覗き見に注意する

パスワードロックをかけた Word や Excel ドキュメントに記録する

○ 覚えるパスワードが 1 つでよい　× スマートフォンに比べて携帯性が低い

POINT
- 他人が開けないように、［文書の保護］→［パスワードを使った暗号化］をする
- 覗き見防止に、パスワードの文字色をグレーなど一目では分かりにくい色に変える
- 紛失に備えて、自分しかアクセスできない外部ストレージ等にバックアップを取る

パソコンのパスワード管理ツール（機器内にのみ格納されるもの）を利用する

○ 覚えるパスワードが 1 つでよい　× スマートフォンに比べて携帯性が低い

POINT
- 紛失に備え、自分しかアクセスできない外部ストレージ等にバックアップを取る

スマートフォンアプリのパスワード管理ツール（機器内にのみ格納されるもの）を利用する

○ 覚えるパスワードが 1 つでよい

POINT
- 紛失に備え、自分しかアクセスできない外部ストレージ等にバックアップを取る

クラウドサービスを使うパスワード管理サービスを利用する

○ 覚えるパスワードが1つでよい
パソコンでもスマートフォンでも
様々なシーンで利用できる

× サービスの品質（セキュリティ、継続性）を
見極めるのが難しい

POINT ●紛失に備え、自分しかアクセスできない外部ストレージ等にバックアップを取る

最適な管理は、いずれのパスワード管理方法であっても、**パスワードをそのまま書かないことです。**例えば、先に述べた「強力なパスワードを使う」で例として挙げたようなパスワードの作成方法を使っている場合、パスワード管理ツールに「basket」と記載されていればどうでしょうか。どんな文章を元に変換したかは、自身の頭の中にしかないので、パスワード管理ツールのデータが漏えいしたとしても問題ありません。繰り返しになりますが、**このように覚えきれないアカウントをパスワード管理ツールなどで管理して、パスワード管理ツールにパスワードをそのまま保存しないことが重要です。**

Tips 6

パスワードの自動入力機能に注意する

Web ブラウザには、パスワードを管理する機能がついています。Web サイトで一度入力した ID とパスワードを記憶するか、利用者に確認し、記憶させると次回以降のアクセス時には自動入力される便利な機能です。

ここで注意すべきは、記憶させた ID とパスワードは、どこに格納され、どうすれば見られるのか、という点です。これらはパソコン、スマートフォンなどの機器内（ローカル）に格納されるため、自分以外も使うパソコンなどでは絶対に記憶させてはいけません。

従来は、パスワードを記憶させた Web ブラウザが動作するパソコンなどの管理をしっかりすれば問題ありませんでした。しかし、最近の Edge、Chrome、Safari（iCould キーチェーン）、Firefox などの Web ブラウザは、クラウドサービスと連携し、パスワード情報をパソコンやスマートフォンなど複数の機器を跨いで共有するようになり、便利になった反面、パスワード情報がどこで、どのように管理されているかわかりにくくなりました。パスワード情報がどこで保管され、どのように利用できるかよく理解しないまま、使うのはやめましょう。

Tips 7

ID 連携トラストフレームワークにご用心

ID 連携トラストフレームワークとは、異なるサービス間で ID と個人情報を連携する取り組みのことです。これを用いて ID 連携する様々なサービスがあり、そのうちのひとつであるソーシャルログインが特に有名です。ソーシャルログインとは、Google や Facebook、Yahoo! とは関係のないサービスで、Google や Facebook、Yahoo! のアカウントで会員登録やログインできるといったサービスのことです。そのサービスと Google などのアカウントを紐づける仕組みで、利用者が持っている Google アカウントの個人情報を共有し、当該サービスのアカウントを作成し、以後のログインにも Google アカウントを利用するので、利用者は新たに ID やパスワードを覚えなくてよいという、非常に便利な機能です。

図 2　ソーシャルログインの例

しかし、このソーシャルログインに見せかけ、アカウントを窃取しようとする手口もあります。ID 連携を行う際は、そのサービスが信頼できるか確認し、よく知らないサービスで使うことはやめましょう。

参考：JPCERT　注意喚起「SNS やクラウドサービスで連携されるアカウント情報には細心の注意を」
https://www.jpcert.or.jp/pr/2015/pr150005.html

2-5 多要素認証（多段階認証）を使う

近年、ID とパスワード以外に、他の要素、例えば事前に配布する乱数表、電話（音声ガイド）、ショートメッセージ（SMS）、スマートフォンアプリ、指紋・静脈・顔認証などを組み合わせ、本人確認をする「多要素認証」（または多段階認証）と呼ばれる技術が広がっています。多要素認証とは、「知っているもの（パスワードなど）」「持っているもの（スマートフォンや IC カード、乱数表など）」「本人自身に関するもの（指紋、静脈、虹彩、顔）」のうち 2 種類以上で認証することで、どれか 1 つを破られたとしてもサービスを利用できないようにするものです。

例えば、Web サービスを利用していて、ID とパスワードによるログインに加え、携帯電話・スマートフォンに SMS で送られた文字列の入力を要求したり、オンラインバンクなどでスマートフォンのワンタイムコード生成アプリで作成された文字列の入力を要求し本人確認をするサービスがこれにあたります。

これにより、パスワードの窃取やスマートフォンの盗難など、多くの情報事故を防ぐことができます。信頼できるサービスが多要素認証を提供する場合には、電話番号の入力が求められることもありますが、積極的に活用しましょう。

2-6 ログイン履歴や変更通知メールを確認する

Google、Microsoft、Yahoo! を始め様々なサービスで、ログイン履歴が確認できるようになっています。ログイン履歴には、ログイン日時、端末情報、ログインをおこなったおおよその位置情報などがあります。あなたのアカウントが窃取され、使用された場合も不審な履歴が残るため、定期的にログイン履歴を確認するようにしましょう。特に日本に在住しているのに外国からのログイン履歴があったり、普段とは違う端末からのログイン記録があったりした場合は、ID とパスワードが窃取されている可能性が極めて高いと言えます。また、こういった不審なログインを機械的に検知してメールや SMS で通知するサービスもあります。

また、アカウントに登録している情報やパスワードを変更すると、登録されているメールアドレスに変更通知メールが届きます。身に覚えのない変更が通知された場合は ID とパスワードが窃取されている可能性が極めて高いと言えます。

このように、**不審なログインや変更があった場合は、すぐにパスワードを変更し、サービス提供元に報告しましょう。**

対策 3

Web

インターネット上の代表的なサービスは、「World Wide Web」（Web、ウェブ）と「メール」です。マルウェアも感染経路として「Web」と「メール」を利用します。「Web」とは、互いにリンクする文書（Web ページ）を公開・共有する仕組みです。Web ページの集まりを「Web サイト」（国内ではホームページと呼ばれることもあります）と呼びます。旧来の Web は検索エンジンと情報を公開するのみでしたが、やがて動きのある Web が多くなり、現在では地図、予約、ショッピング、銀行など生活上の様々なサービスを担うようになりました（Web サービス）。インターネット上のサービスの大部分を占めるため、インターネットそのものだと誤解している人がいるほどです。そして、この Web を閲覧するときに使っているアプリケーションを「Web ブラウザ」と呼び、代表的なものに Microsoft 社の Internet Explorer、Edge、Google 社の Chrome、Apple 社の Safari、非営利のコミュニティ Mozilla が作る Firefox などがあります。

このように Web では様々なサービスが提供され便利になりました。その反面、攻撃手法も巧妙化し、Web サイトが改ざんされ（マルウェアに感染させる仕掛けを埋め込まれるなど）、当該 Web サイトの利用者が閲覧するだけでマルウェアに感染する、広告が表示されたことでマルウェアに感染するといったことがあります。

ここでは、Web を取り巻く脅威を紹介し、その対策について解説します。

なお、Web を運営する教職員は「学校法人立命館情報システム運用管理規程」および関連ガイドラインに従ってください。

Webに関する 6つのポイント

3-1 マルウェア対策をする
3-2 Webブラウザのセキュリティ機能を安易に緩めない
3-3 ダウンロードしたファイルは必ずスキャンする
3-4 Webサイトが本物かどうか確かめる
3-5 詐欺を目的としたWebサイトや広告に注意する
3-6 気になることがあればスキャンする

3-1 マルウェア対策をする

攻撃者の第一目的は、Web サイトやメールを使ってパソコンなどをマルウェアに感染させることです。**Web サイトを安全に閲覧するには、まずはマルウェア対策をすることが大切です**。対策 1「マルウェア（ウイルス）」をよく読んで対策をしてください。

また、OS やセキュリティ対策ソフトには、Web サイトに特化したセキュリティ対策機能を持つものがあります。

例えば、Windows 10 では標準で SmartScreen という機能が動作しています。マルウェアが仕掛けられた Web サイトやフィッシングサイトなどにアクセスしないようにしたり（Internet Explorer、Edge でのみ動作）、ダウンロードしたファイルを自動的にスキャンしたり（Chrome などでも動作）する機能なので無効にしないようにしましょう。

また、市販のセキュリティ対策ソフトの中に、Web サイトの信用評価（Web レピュテーション）、ネットワークを流れるデータパターン（IPS）、Web ブラウザを介して実行されるプログラムのパターン（振る舞い検知）などから危険なサイトを検知して、利用者がアクセスしないよう保護する機能を備えるものもあります。こういった機能のあるセキュリティ対策ソフトを利用するのもよいでしょう。

解説❻

エクスプロイトツール（キット）の脅威

エクスプロイトツール（キット）とは、Web サイトに仕掛けることができるツールで、Web サイトを閲覧しただけでパソコン等がマルウェアに感染してしまいます。エクスプロイトツール（キット）は攻撃者の運営する Web サイトに設置されているだけではなく、Web サイトが攻撃を受けた際に勝手にツールを仕掛けられたり、Web 広告にツールを紛れさせることで他者の Web サイトにリンクを表示させたり（アドバタイジング攻撃）することもあり非常に危険です。さらにこういったツールは、インターネット上で売買されており、今後ますます危険な Web サイトが増えることが予想されます。

エクスプロイトツール（キット）が攻撃可能なソフトウェア（Web ブラウザ、Adobe Flash Player、Java、Adobe Reader、Microsoft Office など）の脆弱性が 1 つでもあれば、マルウェアに感染しますので、OS をはじめとして利用しているソフトウェアの脆弱性対策を徹底するようにしてください。

参考：Kaspersky エクスプロイトとは？なぜそんなに恐いのか？
https://blog.kaspersky.co.jp/exploits-problem-explanation/8327/

3-2 Webブラウザのセキュリティ機能を安易に緩めない

最近では Web ブラウザが標準で Web サイトのセキュリティ対策機能を搭載し、危険なサイトへのアクセスや危険なファイルのダウンロードなどを未然に防ぐケースが増えてきました。**Web ブラウザで何らかの警告が出たら、その警告がどういうものなのかを調べたうえで行動しましょう。**

また、Web ブラウザのセキュリティ対策機能が厳しいため、ある Web サイトが正しく動作しないということがあります。Web ブラウザの設定は、初期状態がメーカーの推奨する設定なので、Web サイトが正しく動作しないなどの理由で、**安易に全体のセキュリティ機能を緩めてはいけません。どうしても必要な場合には、その Web サイトのみに限定したセキュリティ設定を調整しましょう。**一般的に、Web ブラウザのセキュリティ対策により正常動作しない Web サイトでは、FAQ などで設定方法が公開されているので、探してみましょう。

図 3　web ブラウザの設定（Internet Explorer 11）

3-3 ダウンロードしたファイルは必ずスキャンする

インターネットを介して入手したファイルがマルウェアに感染している可能性を疑いましょう。**Web サイトからダウンロードしたファイルは、セキュリティ対策ソフトでスキャンしましょう。**特にパソコンやスマートフォンにインストールするアプリケーション（アプリ）は、スキャンだけでなく、配布元や製造元が信用できるかどうかよく確認しましょう。

Windows 10 であれば、前述の SmartScreen を有効にしておけば、自動でスキャンします。また、パスワード付 Zip ファイルなどの暗号化されたファイルは、暗号化したままではスキャンできないため、暗号化を解除（復号）した後にスキャンするようにしましょう。

3-4 Webサイトが本物かどうか確かめる

金融機関やショッピングサイトなどになりすましてメールでそのサイトに誘導しつつ、ID・パスワード、クレジットカード番号などを入力させる手口が典型的ですが、攻撃者の用意するなりすましサイトは非常に精巧で正規のサイトとの見分けがつきにくくなっています。URL がいつもと違わないか、金融機関などの場合「グリーンバー」が表示されているかなどを確認するようにしましょう。

解説❼

グリーンバー

Web が正規のものであることを証明するためにデジタル証明書を取得しているケースがあります。金融機関などで、URL を表示するアドレスバーが南京錠アイコン＋緑色に表示される場合が有りますが、それを「グリーンバー」と呼びます。これは通常の暗号化を主目的としたデジタル証明書よりも厳格な審査で、その企業が実在しているかなどをデジタル証明書発行機関が確認した上で、発行しているものです。これにより企業の信頼性、URL の正当性、暗号化の保証がされています。

図 4　グリーンバーの例（Internet Explorer 11）

3-5 詐欺を目的としたWebサイトや広告に注意する

Web サイトの利用者の心理に働きかけ、マルウェアに感染させたり、金銭を要求したりする手口も日々巧妙になっています。

例えば、Web を閲覧すると「マルウェアを検知しました」「お使いのパソコンの動作が遅くなっています」「クラッシュ寸前です」などとシステム警告を装う詐欺広告を表示するものがあります。クリックするとさらに不安をあおる内容を表示し、セキュリティ対策、性能改善、修復などのソフトウェア（中身はマルウェア）をインストールや購入するよう誘導されます。類似の広告として「パソコンの動作スピード改善」「スマートフォンのバッテリー不

足改善」など、多くの利用者が感じる不便に付け込んだものもあります。こういったソフトウェアは、マルウェアであることが多いため、対策 1「マルウェア（ウイルス）」をよく読んで、信頼できるソフトウェアのみを使うようにしましょう。

また、こういった表示がどの Web サイトを閲覧しても出る場合、Web ブラウザ以外にも表示される場合は、マルウェアの一種（アドウェア）に感染している可能性が高いでしょう。

金銭を要求する手口として代表的なものが、ワンクリック詐欺です。ワンクリック詐欺とは、Web サイトにアクセスしたり、リンクをクリックしただけで、「会員登録が完了しました」などと表示し、携帯電話やスマートフォンの機種、IP アドレスなどの表示で個人情報を特定していると偽り、「自宅や会社に回収に行く」などと不安をあおってサービス料を不正請求する手口のことです。最近では、アダルト動画サイトなどで、「ゼロクリック詐欺」と呼ばれる亜種的なパターンも発見されています。Web サイト上において契約成立するには、「金額が表示」された上で「利用の意思確認」がなされる必要があります。このような表示がなかったのであれば契約は成立していません。無視をするか、消費者センター等（消費者ホットライン：局番無し 188）に相談しましょう。

参考：東京都　東京くらし WEB 警告表示をして、セキュリティーソフトを購入させる詐欺広告に注意
http://www.shouhiseikatu.metro.tokyo.jp/trouble/trouble25-sagiadvertisement-140106.html

参考：総務省　国民のための情報セキュリティサイト 「ワンクリック詐欺に注意」
http://www.soumu.go.jp/main_sosiki/joho_tsusin/security/enduser/security01/06.html

3-6 気になることがあればスキャンする

前述のとおり、アダルト、出会い系、投資、コンプレックス商法などの誘惑されやすい内容の Web サイトでは、ワンクリック詐欺やエクスプロイトツール（キット）が仕込まれていることが多い傾向にあります。

しかし、悪意のある Web サイトでなくとも、攻撃を受けた Web サイトがマルウェア感染源となるケースがあることも事実で、安全または危険の判断は非常に困難になってきています。（参考 解説 6 エクスプロイトツール（キット）の脅威）

繰り返しになりますが、対策 1「マルウェア（ウイルス）」で説明した通り、OS やアプリケーションのアップデート、セキュリティ対策ソフト導入、定期スキャンやダウンロード時のスキャンを心がけ、容易にマルウェアに感染しないパソコン、スマートフォンにすることが重要です。もし、**怪しい Web サイトに誘導されてしまった、身に覚えのない表示や警告が出たなど、気になることがあれば、パソコン、スマートフォンの全体をスキャンするようにしましょう。**

対策 4

メール

2015 年に発生した日本年金機構の情報漏えい事故に代表されるように、最近報道される情報漏えい事故の多くは「添付ファイルを開いてしまった」「記載されたリンクを開いてしまった」ことがきっかけとなっています。このようなメールは、ますます巧妙になっており、悪意のあるメールかどうかの判別が難しくなってきています。

また、単なる誤送信によって機密情報を流出してしまうといった事故もあります。メールは社会的通信基盤として定着し、電話以上の頻度で使われるようになりましたが、同時に最も情報事故に気を付けるべきコミュニケーションツールの 1 つです。

ここでは、メールを取り巻く脅威を紹介し、その対策について解説します。

メールに関する 7 つのポイント

4-1 迷惑メール（スパムメール）フィルタ設定をする

4-2 添付ファイル、リンクに注意する

4-3 詐欺やフィッシングを疑う

4-4 標的型サイバー攻撃を疑う

4-5 不審なメールを見分けるポイントを理解する

4-6 メールの誤送信に注意する

4-7 機密性の高い情報は書かない

4-1 迷惑メール（スパムメール）フィルタ設定をする

メールを長年使うと、必ずと言っていいほど「迷惑メール（スパムメール）」が届くようになります。ほとんどのメールシステムでは、迷惑メールフィルタ機能を導入し、迷惑メールが届くことを防いでいます。しかし、この機能は大量に流れるメールから、利用者の必要なメールだけを確実に判定できるとは限らず、悪意のあるメールが利用者の受信フォルダに配送されるケース、必要なメールが迷惑メールフォルダに配送されるケースがあります。

まずは、利用するメールシステムに迷惑メール検知機能があるか、自身の設定で作動をONにしているかを確認しましょう。また、誤検知により必要なメールが迷惑メールフォルダに配送されていないか、迷惑メールフォルダの中身を定期的に確認する習慣をつけましょう。

参考：迷惑メール相談センター「迷惑メール対策をはじめましょう」
http://www.dekyo.or.jp/soudan/taisaku/

Tips 8

迷惑メール（スパムメール）を報告する

最近のメールシステムには、「迷惑メールを報告する」機能がついています。逆に「誤検知を報告する」機能もついています。この報告が迷惑メールを分析し、判定するエンジンの学習の一助となりますので、なるべく報告するようにしましょう。

学内のメール環境では、Outlook on the Web（Web メール）を使っている場合のみ迷惑メールを報告することができます。受信トレイなどで迷惑メールとして報告したいメールを選択して、以下の操作をします。

右クリック→［迷惑メールとしてマーク］をクリック

図５　迷惑メールとしてマーク

確認ダイアログが出るので［レポート］をクリックしてください。

図６　迷惑メールのレポート

この操作で迷惑メール報告をした上で、迷惑メールフォルダに移動します。

逆に、誤検知を報告したい場合は迷惑メールフォルダ内のメールを右クリックし［迷惑メールではないメールとしてマーク］をクリックするか、メール本文に表示されている［このメッセージはスパムメールではありません］をクリックしてください。

4-2 添付ファイル、リンクに注意する

メールからマルウェアに感染するケースは、メールに添付されたマルウェアを受信者が開くことで感染するケースと、本文に記載されたURL（HTMLメールのリンク含む）から受信者がWebサイトにアクセスすることでマルウェアに感染するケースがあります。また、アクセスしたWebサイトでID・パスワードを入力するよう促され、ID・パスワードを窃取されるケースもあります。

メールの添付ファイルは、興味本位で開けず、開ける必要がある場合は、一旦パソコンに保存してからセキュリティ対策ソフトでスキャンするようにしましょう。

最近はメールでURLを案内するサービスが多く、見極めが難しいですが、URLや文面をよく見て不審に思うことがあれば、開かないようにしましょう。**URLが差出人と関係のないURLではないか確認することが大切です。**HTMLメールの場合は、リンク偽装（表示されたURL文字列ではないリンク先が設定されている）にも注意しましょう。そのURLが正規のものであるか分からないときは、ブックマークや検索エンジン等で、確実に正規サイトにアクセスできる経路をたどるとより安全です。

誤って添付ファイルを開いてしまったり、リンク先にアクセスしてしまったりしても、対策1「マルウェア（ウイルス）」にしたがって対策をしておくことで感染を逃れられる場合もあります。容易にマルウェアに感染しない環境作りをしていることも重要です。特にOutlook、Thunderbird、Macメールなどのメールクライアントを使っている場合は、メールクライアントの脆弱性を衝くマルウェアもあるため、常にアップデートしましょう。

解説 8

アイコン偽装

Office 文書や PDF のアイコンを模したマルウェアを添付する手口があります。ファイルの種類をアイコンだけで判断している利用者が多いため、誤認識させてマルウェアを実行させるというものです。

一方で、OS は拡張子というファイルの種類を表す文字列（ファイルの末尾につく .docx、.pdf、.jpeg、.exe など）により、どのアプリケーションでファイルを開くか（もしくは直接実行するか）を判断しているため、アイコンと拡張子の違いにより、偽装の有無を確認できます（例えば、画像アイコンなのに .exe というファイル）。最近の OS では、「拡張子を表示しない」ことが初期設定になっている場合がありますので、**必ず拡張子を表示する設定にしましょう。**

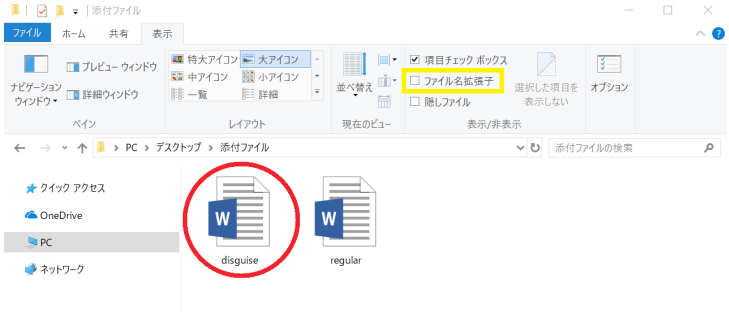


図 7　偽装されたアイコン（ファイル名拡張子を表示しない）

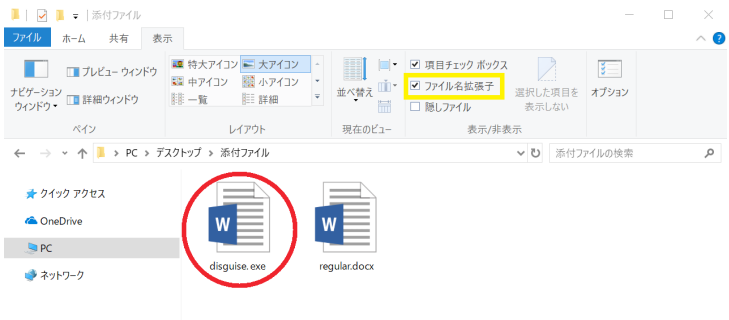


図 8　偽装されたアイコン（ファイル名拡張子を表示する）

最近ではアイコン偽装の派生としてショートカットファイル（.lnk、.url）を添付し、クリックさせることで、マルウェアを仕掛けた Web サイトに誘導する、もしくはそのまま埋め込んだプログラムを実行させマルウェアに感染させるケースが多数報告されています。ショートカットファイルは、スキャンしようとパソコンに保存した際に拡張子が表示されなくなります。見分けるためにはアイコンに右記のような「矢印」がついていないか確認する必要があります。

参考：IPA「ファイル名に細工を施されたウイルスに注意！」～見た目でパソコン利用者をだます手～
http://www.ipa.go.jp/security/txt/2011/11outline.html

4-3 詐欺やフィッシングを疑う

迷惑メール（悪意のあるメール）の多くは不特定多数に送信され、メールの文面で架空請求したり、知り合いや出会いを求める異性を名乗って返信を求めたり、何らかの高価な景品に当選したなど、直接的に詐欺に引込むために使われます。**まず差出人を確認し、信頼できる相手かどうか評価することが大切です**。身に覚えのない相手に連絡したり、安易に誘いに乗ったりしないよう、充分に注意しましょう。

また、フィッシングとは、実在する公的機関や金融機関、企業等を装い、偽の Web サイトに利用者を誘導し、クレジットカード番号、ID・パスワードなどを入力させて窃取する不正行為です。また、ショッピングサイトやネットオークションなどの有名サービスを騙るケースも増加しつつあります。加えて、不審なメールを見分けることは年々難しくなっています。

フィッシングメール事例１「Appleを騙るフィッシング」

■メール文面

Appleをご利用いただきありがとうございますが、アカウント管理チームは最近Appleアカウントの異常な操作を検出しました。アカウントを安全に保ち、盗難などのリスクを防ぐため、アカウント管理チームによってアカウントが停止されています。次のアドレスでアカウントのブロックを解除することができます。

注:アカウントを再開するときは、情報を正確に記入してください。3つのエラーが発生すると、アカウントは永久に禁止されます。このアドレスでアカウントを復元してください:

リカバリアカウント<http://●●●●-suport-appleid.com/>

すぐに復元してください！盗難によるアカウントの紛失を防ぐため、アカウント情報が時間内に確認されない場合、アカウント管理チームはアカウントを完全に凍結します。アカウントを再開する前に、アカウントを再登録しないでください。でなければ、アカウント管理チームはアカウントを凍結することになっております。

今後ともよろしくお願い致します。

Apple サポートセンター

Apple ID | サポート | プライバシーポリシー
Copyright 2017Apple Distribution International, Hollyhill Industrial Estate, Hollyhill, Cork, Ireland. すべての権利を保有しております。

Apple をかたるフィッシング（2018/11/13）

© Council of Anti-Phishing Japan

図９　事例１　メール文面

■リンク先の Web サイト

Apple をかたるフィッシング（2018/11/13）

© Council of Anti-Phishing Japan

図 10　事例１　リンク先の Web サイト

フィッシングメール事例 2「Amazon を騙るフィッシング」

■ メール文面


amazon

タイムセール | アカウントサービス | Amazon.co.jp

アカウント検証

検証番号： 358-0630627-6296026

ご注意ください!

大変申し訳ございません、あなたのアカウントは閉鎖されます。あなたのアカウントAmazonを更新できませんでした、これは、カードが期限切れになったか、請求先住所が変更されたなど、さまざまな理由で発生する可能性があります。

Amazonをご利用いただきありがとうございますが、アカウント管理チームは最近Amazonアカウントの異常な操作を検出しました。アカウントを安全に保ち、盗難などのリスクを防ぐため、アカウント管理チームによってアカウントが停止されています。
24時間以内にあなたの情報を更新しない場合、アマゾンアカウントで何ができるか的を絞ってください。

アカウント検証 <http://securtymanagment-supprt-●●●●.com/>

なぜこのメールを受け取ったのだろうか?
この電子メールは、定期的なセキュリティチェック中に自動的に送信されました。当社はお客様のアカウント情報に完全に満足しておらず、引き続きサービスを継続的にご利用いただくためにアカウントを更新する必要があります。
Amazonカスタマーサービス

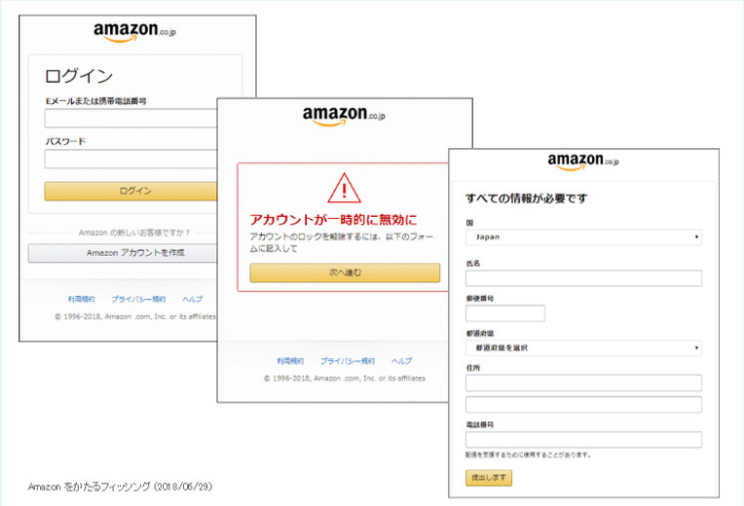
またのご利用をお待ちしております。
Amazon.co.jp

Amazon をかたるフィッシング (2018/06/29)

© Council of Anti-Phishing Japan

図 11　事例 2　メール文面

■ リンク先の Web サイト



© Council of Anti-Phishing Japan

図 12　事例 2　リンク先の Web サイト

参考：フィッシング対策協議会
https://www.antiphishing.jp/

4-4 標的型サイバー攻撃を疑う

2015 年 5 月にあった日本年金機構の 125 万件の年金情報が流出した事故、2016 年 6 月にあった JTB の 793 万件の個人情報流出した恐れがある事故は、標的型サイバー攻撃の名前とともに大きく報道されました。この２件に代表される情報や金銭を窃取する目的で特定の組織（個人）に狙いを定めた「標的型サイバー攻撃」（単に標的型攻撃と呼ぶこともあります）が猛威を振るっています。

「標的型サイバー攻撃」とは、標的とする組織の情報を Web サイト・SNS・電話などで収集し（個人の場合は特に SNS に公開した情報が悪用されます。対策 8「個人情報と権利侵害」参照）、標的とする組織の関連機関や関係者を装って、マルウェアを添付したメールや Web サイトに誘導するメールを送付します。組織内にマルウェアの感染者が出ると、ランサムウェアによる身代金要求にはじまり、そのパソコンを足掛かりに ID・パスワード・目的の情報を窃取しつつ組織内ネットワークの他のパソコンに不正アクセスを試み、最終的には認証システムの管理者権限や基幹システムに保管しているデータを目指し攻撃を続けるという非常に恐ろしいものです。

前述のような「標的型サイバー攻撃」の初手は、攻撃対象のメールアドレスに関係機関を装った巧みな文面のメールを送信することが多く、このメールを「標的型攻撃メール」と呼びます。標的型攻撃メールの特徴は、特定の対象を狙っているため、文面がより巧妙になり、判別が困難になります。本学の教職員が標的となる場合、文部科学省など官公庁の実在の部署名を名乗るメールで添付ファイルやリンク先を確認するように指示する手口が考えられます。このようなメール攻撃による事故は多く発生しており、本学の教職員においても、標的型攻撃メールにより、Web サイトに誘導され、ID・パスワードを入力してしまったことで、ID・パスワードを悪用されたという被害が報告されています。

標的型サイバー攻撃を防ぐには、組織構成員全員がこの標的型攻撃メールを理解し適切に対処することで、マルウェア感染やアカウント窃取などの足掛かりを作らせないことが重要です。パソコンが 1 台でも感染すると学園全体に危険が及ぶ危険性がありますので、十分に注意してください。

標的型攻撃メール事例 1　本学で発生した事例

2016 年 8 月に認証画面や Web サイトなどで周知していた本学メールシステムの更改予定について記載した標的型攻撃メールが多数の教職員を対象に届きました。幸い具体的な被害は確認されていませんが、誘導された Web サイトで ID とパスワードを入力した教職員が数名います。

差出人：大学のメールアカウントのアップグレード〈helpdesk@sso.ritsumei.ac.jp〉
件名：大学のサポート
文面：

注意

現在、電子メールアカウントのすべてのメンテナンス処理を行っています。
これを完了するには、スパイウェア、スパムメールに対するあなたの
アカウントを確認するために、この電子メールにすぐ返信には、次の
リンクを使用する必要があります。

更新するには、ここをクリックしてください
(実際のスパムメールにはこの部分に URL が記載されています)

このプロセスは、あなたがあなたの電子メールを失うことになる、詳細が
提供してあなたは、上記のリンクを持つアカウントを更新しないと、
私たちは、スパムからあなたの電子メールを保護するのに役立ちます

ご理解をいただき、ありがとうございます。

宜しくお願いします、
メールチーム。
管理サービスチームを占めています。

標的型攻撃メール事例 2　文部科学省を騙り大学を標的とした事例

2016 年 5 月にある大学教職員に標的型攻撃メールが届き、文部科学省より注意喚起があった事例です。添付ファイルがマルウェアになっており、差出人は文部科学省のドメインですが、実際には別のメールサーバーに不正アクセスして送信されていたようです。メールの署名は実在する文部科学省職員であり、当該職員が過去に送信したメールが悪用されたとみられています。

差出人：kenjo@mext.go.jp〈*****-saga-saga-saga.com@saga-*****.com〉
件名：【文科省（ご連絡)】新学術領域研究の中間・事後評価について
添付ファイル：中間 - 事後評価に係る様式 20160524.zip

平成 26・27・28 年度採択研究領域の領域代表者各位

お世話になっております。
○○○○○○○○○○○○○○○○○○○○○○○○○○○○○○○

本年度、中間・事後評価のスキームを見直すとともに、
評価報告書の様式の見直しを実施いたしましたので、
来年又は再来年に中間評価又は事後評価を実施することになります
先生方に、本変更点についてご報告させていただきます。
変更点につきましては、添付の事務連絡をご参照ください。

また、
実際の評価時期に作成依頼する際には変更の可能性がございますが、
本年度は使用いたしました様式をご参考までに添付いたします。
特に、今回より追加いたしました別添の " データシート " については、
来年以降は " 全研究期間 " について記載いただくことを予定しておりますので、
現時点よりデータ収集・整理についてご準備いただけますようお願いいたします。

なお、評価に関する例年のスケジュールは以下のとおりとなっております。
5 月半ば　　評価報告書 (添付のもの) の作成を依頼 (領域代表者←文科省)
6 月半ば　　評価報告書の提出 (領域代表者→文科省)
9 月～ 10 月　ヒアリング
12 月～ 1 月　評価結果通知
特に、評価報告書の提出時期と、成果報告書 (様式Ｃ－ 19 及び冊子体の両方)
の提出時期が近接しておりますので、来年は例年 5 月半ばの作成依頼を早めに行い
、
先生方の準備期間に余裕が出るように配慮する予定ではおりますので、
ご対応方よろしくお願いいたします。

今後ともどうぞよろしくお願い申し上げます。

＜本件担当＞

文部科学省研究振興局学術研究助成課
○○○○○○○○○○○○○○○○○○○○
○○○○○○○○○○○○○○○○○○○○

文面：（NHK「かぶん」ブログ http://www9.nhk.or.jp/kabun-blog/200/245719.html より）

4-5 不審なメールを見分けるポイントを理解する

標的型攻撃メールは、受信者が不審に感じない非常に巧妙な文面であるため、「新聞社や出版社からの取材依頼」「官公庁からの通達・注意喚起」など添付ファイルを開かざるを得ない状況になることも考えられます。**メールを確認する際に、差出人・文面・添付ファイルそれぞれに注意をすれば、多くの場合、事故を未然に防ぐことができますので、以下のポイントをチェックしてください。**

〈電子署名（安全なメールの証明）〉

金融機関をはじめ、メールに電子署名する組織が増えています。電子署名とは、メールに認証機関より発行されたデジタル証明書を使ったサインをすることで、差出人と署名者が同一であることを保証し、なりすましでないことを証明する S/MIME という仕組みです。

メールを受信する環境（メールクライアント、メールサービス）によって表示は違いますが、以下のようなアイコンが表示されたり、安全である旨のメッセージが表示されたりすることが多いようです。さらに電子署名されたメールを送信する側の金融機関などでは、電子署名されたメールに関する説明が Web サイトなどで公開されていますので、確認してください。

電子署名アイコンの例

図 13　電子署名アイコンイメージ

また、S/MIME 非対応のメール環境では「smime.p7s」という添付ファイルがついているだけの普通のメールになります。

不審メールのよくある特徴

〈差出人〉

- 差出人に心当たりがない
- 差出人に心当たりはあるが普段とメールアドレスが違う
- 差出人の情報が不足している（名乗らない、署名がない）
- 差出人がフリーのメールアドレスである（Gmail、Yahoo! メール、ドメイン名から組織を判別できない使い捨てアドレス）
- 差出人のメールアドレスと本文内の署名にあるメールアドレスが異なる

〈文面〉

- リンク偽装されている
- 差出人と関係ない URL
- 日本語の言い回しが不自然である
- 日本語では使用されない漢字が使用されている
- 本文だけで内容が完結せず、何らかの行動をさせようとする
- ID・パスワード・クレジットカード番号・個人情報などの入力を求める
- 何らかの危機感をあおる
- 「今すぐ確認を！」「今すぐ電話連絡を！」など緊急性を強調する
- 心当たりのない請求、決済、配送通知
- 実行形式ファイル（拡張子が exe / scr / cpl など）が添付されている
- ショートカットファイル（拡張子が lnk / url）が添付されている
- アイコン偽装されている
- ファイル拡張子が不自然（拡張子が二重になっている、拡張子前に大量のスペース文字など）
- 「fdp.file.scr」→「rcs.elif.pdf」のようにファイル名冒頭に逆さの拡張子がついている（アラビア語等の左右逆に読む言語のための機能（RLO 制御文字）を悪用している）

参考：IPA　標的型攻撃メール＜危険回避＞対策のしおり
http://www.ipa.go.jp/security/antivirus/documents/10_apt.pdf

参考：IPA　IPTA テクニカルウォッチ「標的型攻撃メールの例と見分け方」
https://www.ipa.go.jp/security/technicalwatch/20150109.html

Tips 9

架空請求からの裁判所出廷命令

標的型サイバー攻撃では、個人情報（住所や氏名など）が攻撃者に把握されているケースが少なくありません。攻撃者が、メールによる架空請求を行い、その後、個人情報を利用して実際に訴訟を起こすという手口があります。被告となった利用者が出廷しなければ、原告（攻撃者）勝訴なので「架空請求は無視する」という対策を逆手にとった詐欺といえます。よって、裁判所から出廷命令が届いた場合には、例え架空請求であっても裁判所に確認してください。

参考：法務省 督促手続・少額訴訟手続を悪用した架空請求にご注意ください
http://www.moj.go.jp/MINJI/minji68.html

4-6 メールの誤送信に注意する

メールによる情報漏えい事故の原因には、利用者に届く悪意のあるメールに起因するものばかりではなく、メールの誤送信も多くあります。

メールの誤送信を機械的に防ぐ方法はないため、各自の注意が必要です。ある企業では社員用パソコンに「メール送信前に指差し確認！」というシールが貼られているほどであり、誤送信は個人の注意によってしか防げません。毎日使うツールなので、慣れによる油断が起きやすいものではありますが、スマートフォンによる利用など、メールの利便性が増していく反面、**些細な油断が事故につながることを認識し、送信前には必ず、To・Cc・Bcc とすべての宛先に、本来送信すべきでない宛先がないかを確認するようにしましょう。**

Column 1

転送や差出人変更は控えましょう

メールは日常的に使うコミュニケーションツールですから、慣れ親しんだものを使いたいというのは自然な考え方です。中には、組織（本学）のメールアドレスを使わず、プライベート用のメールアドレスに転送して使う教職員が多くいます。転送は、データ持ち出しと同義ですので、セキュリティ対策の厳しい企業などであれば禁止または許可制にするところもありますが、本学では教育研究の現場での利便性を考慮し、規制していません。ただし、転送先のメールシステムで情報事故があれば、情報漏えいにつながり、個人の責任を問われることもあります。

最近では迷惑メール対策として、送信ドメイン認証（SPF、DKIM）といわれるメールの送信元サーバーと差出人のチェックが厳しくなってきています。安易に転送すると重要なメールが、自分のプライベート用のアドレスに届かなかったり、迷惑メール扱いされたりとコミュニケーションに支障をきたします。

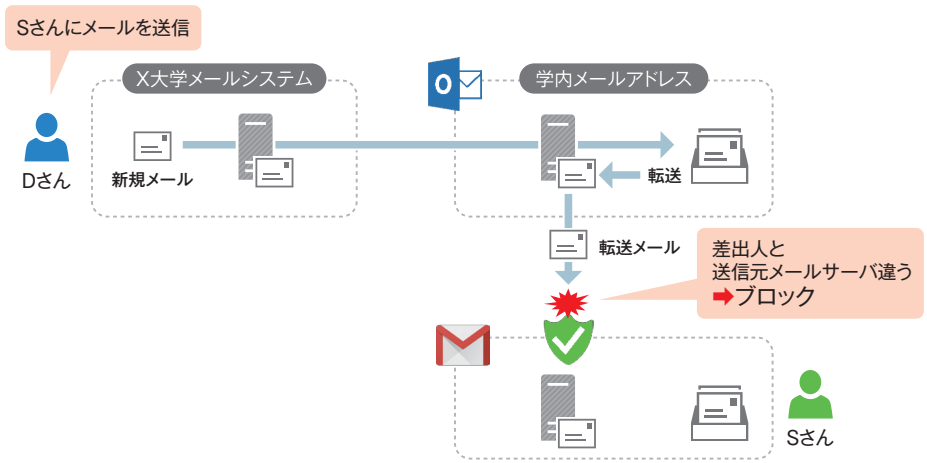


図 14　転送時にメールを紛失する例

また、転送先であるプライベート用のメールアドレスから新規メールを送信したい、返信をしたい、といった場合にメールの差出人を学内メールアドレスに変更して送信することができます。元々、秘書が教授の代理で送信したり、システムが代表アドレスを差出人とするような場合のため、メールの差出人は自由に変更できるようになっています。使い慣れた環境で、学内のメールアドレスを使える（図 15 参照）ため、転送と同様に、使う教職員が多いようですが、この差出人の変更は、悪意のある攻撃者がフィッシングメールや標的型攻撃メールにおいて差出人に「なりすます」メール（なりすましメール、メールスプーフィング）と同様（図 16 参照）であるため、迷惑メールと判定されることが多く、メール紛失の原因となります。

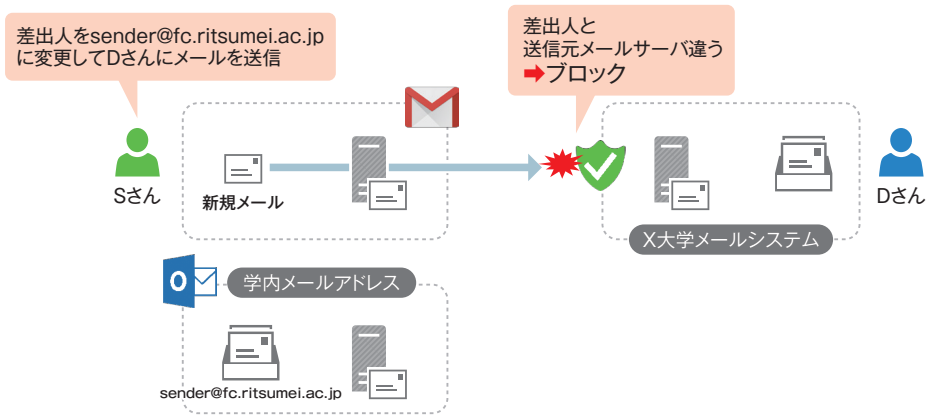


図 15　差出人を変更してメールを紛失する例

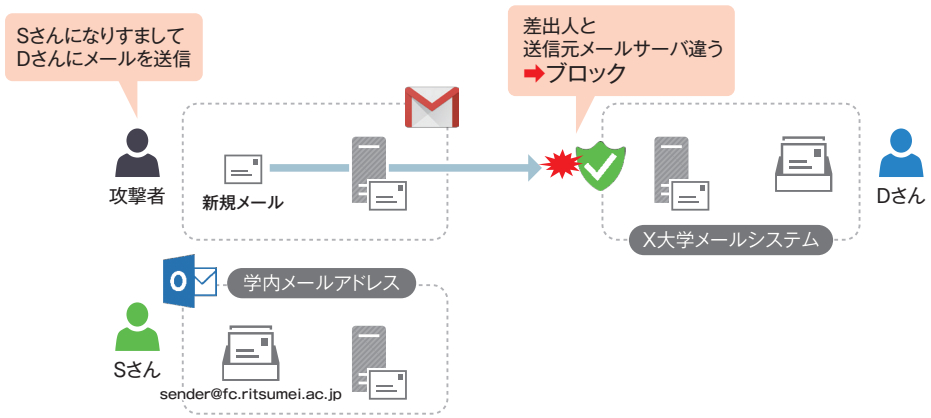


図 16　なりすましメールをブロックする例

近年の迷惑メール対策（特に送信ドメイン認証）により、転送や差出人の変更は、メール紛失の原因となるため、極力使わずに学内のメールをそのまま使うようにしましょう。

4-7 機密性の高い情報は書かない

メールはハガキによく例えられますが、それはメールがインターネット上を通信する際に、誰に盗み見されているかわからないという前提があるからです。（対策 5「通信と保存（暗号化）」参照）。ハガキをポストに投函したのち、悪質な配送作業員が見ているかもしれませんし、配送作業員が目を離した際に覗き見られているかもしれません。インターネットは様々な組織・個人が相互に接続することでネットワークを形成していることから、セキュリティ対策レベルや従業員ガバナンスは必ずしも信用できるものではありません。また、無線による通信が一般化した近年においては、盗聴はより一層身近な脅威となっています。

よって、**盗聴の恐れがあるメールで ID・パスワード、個人情報など、機密性の高い情報は記載したり、添付してはいけません。**メールによるやり取りは、公共の場で話すのと同様に「誰かに聞かれている（見られている）かもしれない」という意識が重要です。

仕組みが難しく敷居が高いのですが、S/MIME や PGP 暗号というメールを暗号化するものもありますので、これらを調べてみるのもよいでしょう。

また、機密性の高い情報（ファイルなど）をネットワーク経由で送付する必要がある場合は、暗号化した上で、適切に管理されたネットワークストレージ（NAS）で受け渡しする、認証機能のついたオンラインストレージの共有機能による受け渡し、ファイル転送サービスを使うようにしましょう。これらの方法については、対策 5「通信と保存（暗号化）」、対策 6「アクセス権（共有）」で詳しく説明します。

対策 5

通信と保存（暗号化）

情報ネットワークの通信経路は、ケーブル、電波、ネットワーク機器、コンピューターなど様々な機器や記憶媒体を通して、データが伝送される仕組みで、利用者にはそのどれを経由しているかが把握できません。中には、適切な管理がなされていない媒体があったり、悪意を持つ管理者が介在する場合もあるため、誰もが判読可能な状態（平文（ひらぶん）といいます）でデータを伝送してしまうと、盗聴により情報が漏えいする可能性があるので、ネットワークに接続する機器の使い方や設定に気をつけましょう。

また、パソコン、ストレージ機器、USB メモリ、SD カードなどの機器や記憶媒体を廃棄した場合、盗難に遭った場合、紛失した場合などに、データが平文で保存（記録）されていると機器や記憶媒体のデータが復元可能になるため、第三者が機器や記憶媒体を入手すると情報が漏えいする可能性があります。

これらの情報漏えいを防ぐためには、平文のデータを通信経路、機器、記憶媒体で暗号化し、盗聴や記憶媒体の入手が可能であっても、データの中身がわからない状態にすることが有効です。

ここでは、通信や保存時のデータにおける情報漏えいのリスクを紹介し、その対策である暗号化について解説します。

暗号化に関する 4つのポイント

5-1 Webサイト利用時の暗号化を確認する

5-2 メールは暗号化されず配信されることを意識する

5-3 無線LAN（Wi-Fi）利用時の設定を確認する

5-4 機密性の高いデータを暗号化する

5-1 Webサイト利用時の暗号化を確認する

Web サイトの URL は http:// と https:// から始まる 2 種類があり、http は平文で Web サイトと通信すること（HTTP 通信）を、https は暗号化して Web サイトと通信すること（HTTPS 通信）を表しています。かつては HTTP 通信が主流でしたが、近年では HTTPS 通信の方が主流になり、スマートフォンなどモバイル端末のアプリでは HTTPS 通信を必須とするような時勢になっています。

HTTPS 通信をする Web ブラウザをはじめとするアプリケーションは、まず認証機関により発行されたデジタル証明書を使い、Web サイトが詐称されていないか認証し、次に暗号化通信をする仕組みになっています。少し分かりづらいかもしれませんが、**利用者として意識すべきは、HTTPS 通信になっているか、デジタル証明書は信用できるかという 2 点です。**

まず 1 点目は、HTTP 通信になっている Web サイトで、重要な情報（ID・パスワード、クレジットカード番号、個人情報など）を入力してはいけません。Web ブラウザではアドレスバーに南京錠のアイコンが表示されている（HTTPS 通信をしている）ことを確認しましょう。

HTTP 通信

図 17　HTTP 通信（Internet Explorer 11）

HTTPS 通信（一般の証明書）

図 18　HTTPS 通信（Internet Explorer 11）

また、南京錠が表示されていても偽のデジタル証明書の場合、Web ブラウザが信用する認証機関として登録されていない場合やデジタル証明書の有効期限などの不備のある場合など、Web ブラウザが警告画面を表示することがあります。警告が出ている場合、別サーバーに誘導されていたり、盗聴されているなど、安全ではない可能性があるので、注意しましょう。

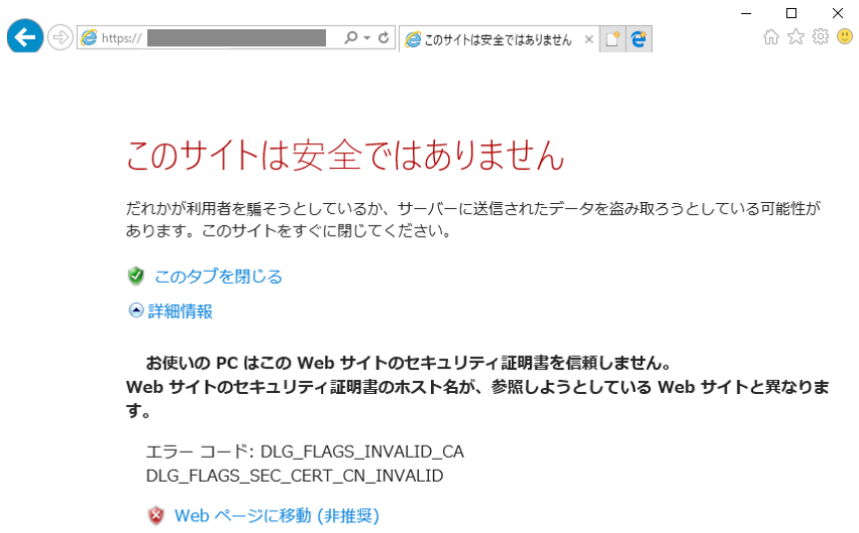


図 19　証明書に不備がある場合の警告（Internet Explorer 11）

2 点目は、一般のデジタル証明書は利用者がアクセスした URL が示す Web サイトに確実にアクセスできていることを保証しますが、その Web サイトが利用者の想定する Web サイトであることまで保証するものではありません。

デジタル証明書はドメインの管理者であれば取得できるため、悪意のある攻撃者が実在する組織名と紛らわしい（例えば ritumei.jp というような）ドメインを取得して、Web サイトのなりすましを行うことができます。よって、HTTPS 通信であっても URL が目的の組織が提供する Web サイトかどうか、確認する必要があります。

また、金融機関などでは安全性を示すため、実在確認などの厳正な審査結果を証明する EV 証明書というものを取得するケースが増えています。その場合、アドレスバーが緑色になり（グリーンバー）、南京錠マークの横に社名が出るようになります。それにより、URL

の安全性がより簡単に確認できます。

HTTPS 通信（EV 証明書＝グリーンバー）

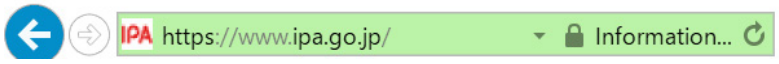


図 20　グリーンバー（Internet Explorer 11）

5-2 メールは暗号化されず配信されることを意識する

メールは、インターネット創成期からあるサービスであり、世界中に無数のメールシステムが存在し、かつ暗号化非対応のものが多く残っています。メールはこれら無数の暗号化非対応のメールシステムを経由して配送されるため、常に配送経路上に非暗号区間が存在します。前述の通り、インターネット上での通信は、どこで盗聴されているかわからないという前提に立って利用する必要があります。（対策 4「メール」も参照）

ただし、利用者が自分で暗号化できる区間もあります。それはパソコン、スマートフォンなどメールを閲覧する機器から、自身のメールアドレスを管理するメールサーバーの間です。この区間は、あなたのメールボックス内にあるデータがすべて流れる区間です。攻撃者があなたを標的にした場合、この区間が一番危険と言えます。さらに無線通信が盗聴される危険性のある区間でもあるので、暗号化されているか必ず確認しましょう。

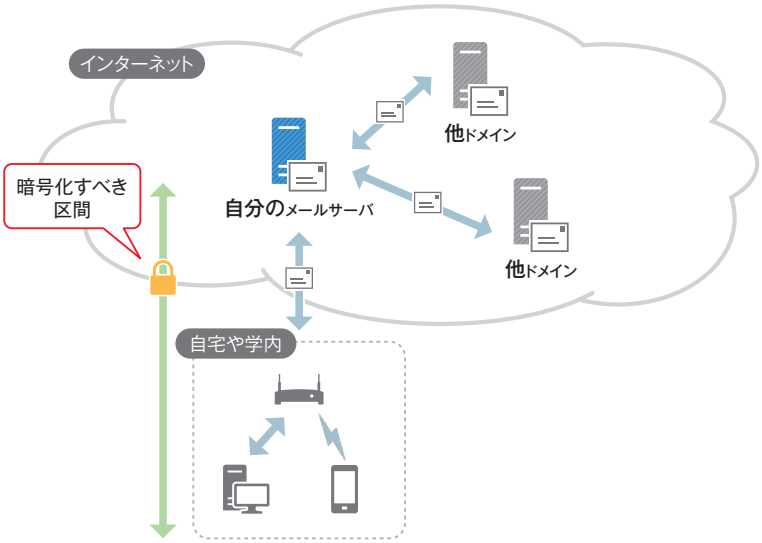


図 21　メールの配送経路

Web ブラウザでメールを送受信する Web メールの場合は、前述の「Web サイト利用時の暗号化を確認する」を参照してください。メールクライアントを使って送受信する場合は、接続方式の設定を確認して POP/IMAP/SMTP となっていれば、平文でメールが送信されてしまうため、POPS/IMAPS/SMTPS など暗号化された接続方式の設定に変更しましょう。

5-3 無線LAN（Wi-Fi）利用時の設定を確認する

近年では、学内や自宅だけではなく、駅、空港、ホテル、カフェ、携帯キャリアの提供する Wi-Fi スポットなど（公衆無線 LAN やパブリックネットワークと呼びます）に接続することも多くなりました。また、自宅において無線 LAN（Wi-Fi）を利用するために無線 LAN ルーター（Wi-Fi ルーター）や無線 LAN アクセスポイント（Wi-Fi アクセスポイント）も利用者自身が設定することが増えてきました。

「接続する」場合も「接続される機器を設定する」場合も注意すべき点は、基本的に同じです。まず、無線 LAN（Wi-Fi）の通信は、通信の状態によって盗聴・解読され、機密性の高い情報が悪意のある第三者の手に渡ってしまう可能性があることを認識しましょう。**特に学内や公共の場で無線 LAN（Wi-Fi）に接続するときは、通信が暗号化されているので大丈夫と誤解しがちなので、気をつけましょう。**

表 1　通信の状態と盗聴・解読される危険性

通信の状態	盗聴・解読
暗号化されていない	非常に危険
セキュリティキー（パスワード）が公開・共有されている	危険性あり
解読方法の公開された暗号化方式を使っている	危険性あり
最適な暗号化方式を使っている	安全

まずは接続する機器で、通信の状態を確認する方法として次のようにすれば確認できます。

1. 接続する機器の無線 LAN（Wi-Fi）設定を確認して「南京錠マーク」や「セキュリティ保護あり（＝暗号化されている）」という表記があれば暗号化されています

2. 学内も含めて公共の場で提供されているものは、セキュリティキー（パスワード）公開・共有されています
3. 暗号化方式は、接続する機器の無線 LAN（Wi-Fi）設定の詳細を確認して、WPA2-PSK となっていれば、問題ありません（将来的には WPA3 に変わっていきます）

解説⑨

無線 LAN（Wi-Fi）のセキュリティキー

読者がイメージしやすいようにセキュリティキー（パスワード）と表記していますが、厳密には無線 LAN（Wi-Fi）の利用可否を判断するための合言葉としてのパスワードではありません。セキュリティキーは、無線 LAN 通信の暗号化のためにかける鍵として使います。誰もが同じ鍵で通信するため、学内や公共の場で同じ鍵を持っている人同士であれば、傍受した通信を解読できてしまいます。

自宅など限られた利用者しか、セキュリティキー（パスワード）を知らない環境で、適した暗号化方式を使えばよいのですが、学内や公共の場ではどのようにすればよいのでしょうか。Web を例にすると、対策 5-1「Web サイト利用時の暗号化を確認する」ができていれば問題ありません。なぜなら、無線 LAN（Wi-Fi）でいう暗号化は、Web サイトで使う暗号化である HTTPS 通信をさらに暗号化しているものだからです。ただ、機器のすべての通信を把握して、安全が確保されていることを確認するのは困難ですので可能なら VPN を使いましょう。

解説⑩

VPN とは

VPN（Virtual Private Network）とは、自宅や公衆無線 LAN などでインターネットに接続しているパソコンやスマートフォンなどを、組織で用意されたネットワークの入口まで暗号化し、組織内でネットワークを利用しているのと同等の安全性を確保する仕組みのことです。

フリー Wi-Fi スポットやホテルなど公衆のネットワークが暗号化されていない場合、VPN を使うとすべての通信を暗号化することができます。

次に利用者自身で無線 LAN ルーター（Wi-Fi ルーター）などの機器を設定する場合について注意すべき点を解説します。基本的に前述の「接続する」場合の逆で以下の通りです。

1. セキュリティキー（パスワード）を設定しましょう
   （20 文字以上の推測しにくい文字列を推奨）
2. セキュリティキー（パスワード）を不用意に教えてはいけません。機器のボタンによる接続の仕組みなどを活用しましょう
3. 暗号化方式は WPA2-PSK 対応にする
4. 機器の管理者パスワードなどを初期設定から変更し、管理画面へのアクセス制限をしましょう

Column 2

無線 LAN（Wi-Fi）同士の干渉

セキュリティ対策とは直接関係ありませんが、無線 LAN（Wi-Fi）は限られた周波数帯域が決められており、その中でしか利用できません。教育研究用の無線 LAN 網を学園全体に整備するため、限られた周波数帯域において電波干渉が起こらないように配置しています。しかし、独自に設置された無線 LAN ルーター（Wi-Fi ルーター）をはじめとした別の無線 LAN（Wi-Fi）環境があると、電波干渉し、他の教員・学生に迷惑がかかるということもありますので、学内無線 LAN が利用可能な場所ではなるべく無線 LAN ルーター（Wi-Fi ルーター）を設置しないでください。

5-4 機密性の高いデータを暗号化する

データを格納する機器・記憶媒体は、パソコン、ストレージ機器、USB メモリ、SD カードなど様々な種類があり、そのそれぞれに廃棄、盗難、紛失などにより第三者の手にデータが渡ってしまう可能性があります。こういった場合においても、データが暗号化されていれば、情報漏えいを防止することができます。

データを暗号化する方法は色々あります。主なものは「機器やフォルダなどを暗号化する」「USB メモリや SD カードなど可搬記憶媒体を暗号化する」「Office 文書、PDF、圧縮ファイル（zip ファイルなど）などを暗号化する」の 3 つです。

一つ目は、パソコンやスマートフォンでは、OS 標準機能や商用の暗号化ソフトによるストレージの暗号化ができます。機器（ストレージ全体）、アカウント、フォルダなどの単位で暗号化ができます。USB 接続のストレージやネットワークストレージなどの機器では、暗号化機能を有した製品があります。盗難、紛失、廃棄などで機器を入手した第三者は、機器を分解し、内部のストレージ（ハードディスクや内蔵メモリなど）に直接アクセスすることで、ログインなどの OS の認証に関係なく、データを窃取することができますが、暗号化されていればデータの中身を知ることはできません。情報漏えいを防ぐため、機密性の高いデータを格納する機器では、暗号化しましょう。

各 OS の暗号化方法

■ Windows 10

［スタートボタン］ › ［bit と入力］ › ［BitLocker の管理］
BitLocker という機能を使ってドライブを暗号化します

■ macOS

［システム環境設定］ › ［セキュリティとプライバシー］ › ［FileVault］
FileVault という機能を使ってアカウント単位で暗号化します

■ iOS

iOS はすべて暗号化されています

■ Android

［設定］ › ［ロック画面とセキュリティ］ › ［機器の暗号化］

ただし、これらの暗号化ソフトを利用する際には復旧用のキーを確実に保管しましょう。この復旧用のキーがないと、OS リカバリや初期化できないことがあります。

二つ目に、USB メモリ、SD カード、書込み可能な CD/DVD など、可搬記憶媒体もデータを持ち運ぶ場合、受け渡しする場合などの紛失、盗難、またはデータを削除せずに廃棄するなどで、情報漏えい事故につながります。こういった可搬記憶媒体についても OS 標準機能（BitLocker や FileVault）や商用の暗号化ソフトにより、暗号化することが可能です。また、USB メモリ自体に暗号化機能がついているものもあります。可搬記憶媒体は管理をきちんとすることが最も重要ですが、機密性の高いデータを格納する際は、万一に備えて暗号化するようにしましょう。

最後に、Word や Excel などの Office 文書、PDF、zip などで複数ファイルを圧縮する場合などは、それぞれのアプリケーションの機能を使い暗号化することができます。特にオンラインストレージなどのクラウドサービスにデータを預ける（保存する）場合は、ID・パスワードの窃取や共有設定の誤りなどで、情報漏えいする可能性もあります。そういった場合に備え、機密性の高いデータは暗号化したものを預ける（保存する）ようにしましょう。

対策 6

アクセス権（共有）

アクセス権とは、機器・データを利用する権限のことです。ICT が身近になり、様々な機器がインターネットに接続され、SNS、カレンダー、ファイルなど多様な情報がインターネット上のサービスで「共有」できるようになりました。SNS の公開範囲、カレンダーの共有、ファイルの共有などの設定をするということは、あなたの情報を共有する範囲を設定する、つまり、誰にアクセス権を与えるかを設定することになります。また、自宅で無線 LAN（Wi-Fi）を使えるようにした際にアクセスポイントの設定をするのも、自宅のネットワークにアクセスしてよい人や機器を決めているわけですから、アクセス権の管理にあたります。**もはや、アクセス権の管理は専門家だけがするものではありません。インターネットを利用するすべての人が意識し、責任をもって管理する必要があります。**「誰がその情報にアクセスしてよいか」を意識せずにインターネットや機器を利用すると必ず大きな情報事故につながります。特に、インターネットに一度流出した情報は、完全に削除したり回収したりすることはできません。まさに取り返しのつかない事態に陥ります。

SNS やオンラインストレージなどの利用時には、常日頃からどのような情報をどこまで共有してよいかを意識してアクセス権を与えるかどうかの判断をしなければなりません。確認を怠って情報の発信や共有をするということは、車の運転で必要な安全確認を怠るのと同じように、大きな事故につながります。

ここでは、データを共有する際のリスクについて紹介し、その対策を解説します。

共有に関する 3つのポイント

6-1 パソコンのファイル共有に注意する

6-2 クラウドサービスでの共有機能に注意する

6-3 ネットワークに接続するすべての機器の設定に注意する

事例❷

Google グループの初期設定問題による情報漏えい

2013 年に消費者向け（コンシューマ向け）サービスである Google グループを業務利用した複数の官公庁、大学など、多数の機関での情報漏えい事故が発生したことが報道されました。Google グループの初期設定が一般公開であったため、関係者外秘の情報がインターネットに公開されてしまったのですが、Google 社が悪いわけではなく、一般的にこのような消費者向けサービスでは、情報を広く公開・共有する傾向にあり、問題は、利用者がアクセス権を確認していなかったことに起因し、意図しない人に情報が公開されたというものです。

利便性のみを優先し、アクセス権などの設定を確認せずに、安易な気持ちで消費者向け（コンシューマ向け）サービスを教育・研究・管理運営などの業務に使うことは避けましょう。

参考：IPA インターネットサービス利用時の情報公開範囲の設定に注意！
https://www.ipa.go.jp/security/txt/2013/10outline.html

6-1 パソコンのファイル共有に注意する

パソコンには様々なアクセス権の設定があり、非常に複雑です。特に注意する必要があるのはファイルの共有設定です。基本的に自分だけがアクセスできるようにしておき、必要なときに限られた相手に対してのみ許可しましょう。また、共同作業が終わった際には、共有設定を削除するようにしましょう。誰でも書込み可能にしておくと、ネットワーク攻撃の入口になったり、マルウェアの拡散の原因になったり非常に危険です。**ファイル共有するときは相手を限定する、使い終わったら設定を削除することを習慣化しましょう。**

6-2 クラウドサービスでの共有機能に注意する

Dropbox、Google Drive、iCloud、OneDrive、Yahoo! ボックスなどオンラインストレージと呼ばれるサービスにファイルを預ける（保存する）利用者が増加しています。インターネットに接続できる場所ならどこでもアクセス可能で、パソコン、スマートフォンなど様々な機器からアクセス可能であるため、非常に利便性が高いサービスです。オンラインストレージは、簡単にファイル共有ができるため、ファイルの受け渡しにもよく使われます。オンラインストレージを利用するにあたって重要な注意が２つあります。

第一に、ほとんどの消費者向け（コンシューマ向け）のオンラインストレージは標準の共有方法として、インターネットに全公開される（解説 11「URL 公開機能」参照）ため、オンラインストレージの共有機能は、パソコンのファイル共有よりも一層の注意が必要です。共有相手をどのように制限するのか、設定時の公開範囲を必ず確認し、相手が受け取り次第すぐにファイルを削除するか共有設定を変更するようにしましょう。また、**インターネットに全公開する共有機能しかないサービスで、機密性の高いデータを共有してはいけません。**機密性の高いデータを共有する場合は、認証による特定個人に限定可能なサービス、かつ多要素認証、ログイン履歴、変更通知メールなど認証に関するセキュリティ機能（対策２「IDとパスワードの管理」参照）がしっかりしたサービスを選びましょう。また、利便性は損なわれますが、接続元ネットワークを制限することも非常に有用です。

第二に、データを共有することで、共有相手にどのような権限を与えるのかを必ず意識しましょう。多くの場合、共有時に相手に与える権限は、参照、編集、再共有になります。再共有とは、共有相手がさらに第三者に共有する権限を与えることです（図 22 参照）。誰かに共有した時点で「人の口に戸は立てられぬ」というように、情報漏えいを防ぐことは難しくなりますが、共有相手の権限を適切に設定することで、誤編集、改ざん、紛失などを避けることができます。よって、**どの操作で共有相手にどのような権限がつくのかを確認し、共有時には必要な権限だけを渡すようにしましょう。**

図 22　再共有

また、ファイルを預けるオンラインストレージが最もリスクが高いと言えますが、SNS、カレンダー、動画や写真の保管サービスなど「データを預ける」「共有する」Web サービス全般で注意しましょう。

事例❸

オンラインストレージの危険性

学内にあるネットワークストレージ（ファイルサーバー）と学外にあるオンラインストレージはセキュリティの観点から大きく違うところがあります。それはネットワークです。

学内のネットワークは、学内構成員以外はアクセスできませんが、オンラインストレージは、インターネット上に公開され、悪意をもった攻撃者にアクセスされる可能性があります。

例えば、2016 年秋にある大学で発生した情報漏えい事故では、職員がフィッシングメール（または標的型攻撃メール）により、ID・パスワードだけでなく、オンラインストレージに預けていた業務情報も窃取され、さらに当該職員のメールアカウントを踏み台にして、12 万通もの迷惑メールが送信されました。

機密性の高い情報は、適切なアクセス権を設定した上で、学内のネットワーク制限を施した安全な場所に保管すべきです。利便性を考慮し、学外にあるオンラインストレージを利用する場合は、接続元ネットワークを制限するなどの対策が必要です。もしくは、対策 2「ID とパスワード」で紹介した「多要素認証」を使ってもよいでしょう。

解説11

URL 公開機能

オンラインストレージ、カレンダー（Google Calendar など）、動画サービス（YouTube）などのサービスでは、非公開 URL や限定公開 URL など呼び名は違いますが、URL を知っている人にだけ公開する機能があります。その仕組みは、人にもコンピューターにも予測が困難な URL を生成し、利用者が共有したい人にだけ、その URL を教えることでデータを共有できるというものです。

一見、安全なデータ共有方法に思えますがよく考えてみると**URL を知っている人は、世界中の誰であれアクセスできるわけですから、アクセス権を設定しているとは言えません。**家の鍵をわかりにくい場所に隠して渡すようなものです。URL を記載したメールが漏えいしたり、共有相手が URL を漏えいしたり、SNS に安易に書き込んだりすることで URL が拡散する可能性があり、機密性の高い情報に使う機能ではありません。

※ Google カレンダーは、非公開 URL という機能名で、URL を知っている人は誰でも参照可能なので注意が必要です。この URL は変更できますが、公開を停止することはできません。予定単位でアクセス権を設定しましょう。

Column 3

ファイル転送サービスの選び方

大きなファイルを送受信するとき、機密性の高い情報を含んだファイルのやり取りをするときに宅ファイル便、Giga File 便、データ便などの「ファイル転送サービス」と呼ばれるサービスを使うことがあります。Web サイト上にファイルを預け、生成された URL を共有する仕組みです。機密性の高い情報を送付する場合、セキュリティの面で 3 つ意識すべきことがあります。

まずは、パスワード機能がついており、パスワードがメールなどで自動送信されずに、パスワード送付方法は自分で選択可能なものが良いといえます。パスワードは、電話、FAX、SMS、Skype や LINE などのメッセンジャーなど、ダウンロード用 URL を通知するメールと別経路で送付することで、安全性を確保できます。

次に、アップロードやダウンロードをおこなった日時、場所の履歴が確認できるサービスを利用するようにしましょう。これにより、身に覚えのない時間や場所で該当ファイルにアクセスした履歴を発見することができるため、情報漏えいを察知することができます。

最後に、こういったサービスでは利用者は「データを預けている」わけですから、預けたデータがどのように取扱われるのかを確認する必要があります。サービス提供者がはっきりしている、利用者評価が高いといったことに加え、「サービス規約」を必ず確認しましょう。サービス規約の確認ポイントについては、対策 9「サービス提供者との取り決めを確認する」を参照してください。

6-3 ネットワークに接続するすべての機器の設定に注意する

対策 1-3「ネットワークに接続するすべての機器をアップデートする」で述べたのと同様に、ネットワークに接続するすべての機器でアクセス権を中心とした設定に注意する必要があります。ネットワークに接続する機器は、パソコン、スマートフォン以外にも、無線 LAN ルーター（Wi-Fi ルーター）、ネットワークストレージ（NAS）、プリンタや複合機、ネットワークカメラ（監視カメラ、Web カメラなど）や TV 会議システム、大型モニタ、プロジェクタ、デジタル家電（テレビ、HDD レコーダー、家庭用ゲーム機など）、様々なものがあります。それぞれネットワークやアクセス権を適切に設定する必要があります。

無線 LAN ルーター（Wi-Fi ルーター）の設定は、対策 5-3「無線 LAN（Wi-Fi）利用時の設定を確認する」を参照してください。

ネットワークストレージ（NAS）は、前述の対策 6-1「パソコンのファイル共有に注意する」と同様にファイル共有相手を限定し、ID 管理を適切に行ってください。誰でも参照可能・書込み可能にしてはいけません。**ネットワークストレージ（NAS）のインターネット公開機能を利用して、機密性の高い情報を共有してはいけません。**利便性の観点から、どうしてもインターネットを経由して共有する場合は、接続元ネットワーク制限やアクセス制限など適切な制限をおこなってください。また、最近では、メディア共有やインターネット公開など様々な機能がついていますので、マニュアルをよく読んで不要な機能をオフにしましょう。

事例 4

ネットワークストレージによる情報漏えい事故

2014 年にある大学で、教員が３万人以上の学生名簿や３千人以上の成績データの入ったネットワークストレージを持ち帰り、自宅のネットワークに接続しました。このときに設定をよく確認しなかったために、データがインターネット上に公開されました。しかも、公開されたデータは、検索エンジンに取得され、内容がインターネット上で検索できる状態になりました。

取り扱う情報の重要性、責任やセキュリティに対する意識をしっかり持っていれば、そもそも学外へ持ち出すということもなかったのではないでしょうか。

プリンタや複合機では、データ保存領域がありますので脆弱性対策やアクセス権の管理をしなければ、プリントやスキャンした文書が流出することがあります。

Web カメラや防犯カメラも脆弱性対策やアクセス権の管理をしなかったために、映像が流出するという事件が発生しています。

他にも様々なものがインターネットに接続するようになっていますので、パソコンやスマートフォンだけではなく、ネットワークにつなぐものを利用する場合は、すべて本書の対象と考え、対策 1-3「ネットワークに接続するすべての機器をアップデートする」で紹介したファームウェアの更新に加えて、アクセス設定（特に管理画面のアクセス権）を確認して、適切な管理をしてください。

参考：IPA 複合機やウェブカメラ、情報家電などにも適切なアクセス制限を
https://www.ipa.go.jp/security/announce/20150317-netdevice.html

対策 7　スマートフォンなどのモバイル端末

機器の軽量化や公衆無線 LAN 環境の拡充により、移動中や外出先で、スマートフォン、タブレット、軽量小型のノートパソコンなど、容易に持ち運ぶことができる「モバイル端末(デバイス)」と呼ばれるコンピューターに触れる機会が増えてきました。基本的にはインターネットに接続するコンピューターですので、パソコンと同様のセキュリティ対策が必要になります。したがって、モバイル端末についても、まず対策 1「マルウェア（ウイルス)」を実施してください。

ここでは、スマートフォン、タブレット、軽量小型のノートパソコンなどのモバイル端末ならではのリスクを紹介し、その対策について解説します。

モバイル端末に関する 2つのポイント

7-1　盗難・紛失時も情報にアクセスされない工夫をする

7-2　アプリへのアクセス許可やID・パスワード提供に注意する

7-1　盗難・紛失時も情報にアクセスされない工夫をする

モバイル端末は、持ち歩くことによる盗難・紛失の恐れがあります。**盗難されない、紛失しないように注意することは当然ですが、盗難・紛失が発生する前提で、事前に対策をしておくことが重要です。**

まず、メールを含め、機密性の高い情報にアクセスする機器では他人が使えないようにロックまたはユーザー認証設定をしてください。また、パターンロックや暗証番号は、単純なものにしない、かつ人に見られないことが重要です。スマートフォンでは指紋や皮脂汚れでパターンや番号が見えてしまうので、画面の汚れはこまめに拭くようにしましょう。

次に、OS、携帯キャリアのオプションサービス、セキュリティ対策ソフトでは盗難・紛失時用の GPS 追跡機能などがあるので、利用できるサービスを確認し、事前にリハーサルしておきましょう。さらに、追跡だけでなく、いざという時にモバイル端末をリモートでロックする機能や、パスワードを変更する機能、紛失したモバイル端末からサービスへの接続を停止する機能、リモートからデータを消去する（リモートワイプ）機能などの使い方を確認し、設定を有効にしておきましょう。iOS や Android などのモバイル用 OS だけでなく、Windows 10 や macOS にも同様の機能があります。

ノートパソコンでは、必ずユーザー認証を有効にし、起動しただけでは使えないようにします。また、ドライブ（ハードディスクや USB メモリなど）を抜き取ってデータを読み込むという手口もありますので、機密性の高い情報を格納したりアクセスしたりするモバイル端末では必ずドライブの暗号化をしてください。（対策 5-4「機密性の高いデータを暗号化する」参照）

また、むやみに機密性の高い情報のデータを格納して持ち歩かない、ダウンロードしない（したら削除する）ことで、盗難・紛失時に流出する情報量が少なくなるようにしましょう。

事例❺

情報漏えい事故における盗難・紛失の割合

JNSA の情報セキュリティインシデントに関する調査報告書では、事故原因において、盗難・紛失は以下のような割合と報告されています。

表 2　JNSA 情報セキュリティインシデントに関する調査報告書

調査年度	紛失・置忘れ	盗難	計
2014	12.6 %	3 %	15.6 %
2015	30.4 %	5.5 %	35.9 %
2016	13.0 %	5.3 %	18.3 %

※ USB メモリなども含まれている

教育機関では取り扱う個人情報が多く、実際に複数の情報漏えい事故が発生しています。本学園でも 2007 年、2012 年と空き巣や車上荒らしにより、個人情報が流出する事件がありました。

7-2 アプリへのアクセス許可やID・パスワード提供に注意する

スマートフォンやタブレットの OS である iOS、Android、Windows 10 では、機器に格納される利用者の情報や機能にアプリがアクセスしてよいかを管理する設定機能があります。アプリのインストール時や初めての起動時に、電話 / 通話、ストレージ、アドレス帳（連絡先）、アカウント、他のアプリ、位置情報、ネットワーク、SMS または MMS などへのアクセスを許可するか確認があります。これらをよく読まずに許可するのではなく、自分のどんな情報が読み取られているのかをよく確認しましょう。

また、スマートフォンアプリには他のサービスの ID・パスワードを入力することで、正規のサービスに比べ、より高い利便性を提供することを売りにするものがあります。これらのなかには、オンラインバンク、クレジットカード、電子マネーなど金銭取引に直結するアプリも多くあります。例えば、銀行の口座取引情報、クレジットカードの利用情報、電子マネーの利用情報などをまとめて管理したり、家計簿に取込んだりするようなアプリです。こういったアプリでは、その製作者に自分の利用する銀行や信販会社の情報を提供（または情報管理委託）していることになりますので、決して利便性だけに目を向けず、銀行やクレジットカード会社が正式に認めているアプリなのか（Tips 7「ID 連携トラストフレームワークにご用心」参照）、そのアプリ提供者が信頼のある企業なのかをよく確認しましょう。

Column 4

大学・附属校が提供していないサービスやアプリ

近年、学生団体や学生個人、あるいは学外組織が、学生向けのサービスやアプリを提供する事例が増えてきました。このような活動自体に法律上の問題はありませんが、このようなサービスやアプリの傾向として、大学・附属校が提供するサービスの利便性の低さをカバーしたり、あるいは大学・附属校が提供する複数のサービスを 1 つに集約することなどを目的とし、本学の ID・パスワードでログインさせ、アプリを通じ、公式サービスにアクセスする仕組みを利用するものが多くなっています。

こういったアプリでは、入力した ID・パスワードやそのアカウントでアクセスしたあなたの情報がモバイル端末外に格納されていないか、アプリ提供者などの利用者以外の者がそれらの情報を取得できない仕組みになっているか、確認することができません。

そのほかにも、サービスやアプリの提供者の責で利用者が誤った情報を受け取る、提供者の責に起因するものでなくともサービスやアプリの脆弱性があり、サイバー攻撃により情報が漏えいするといったリスクもあります。

これらのリスクを考えると、ID・パスワードが発行されるサービスを、その提供者が認めていない第三者のサービスやアプリから利用するべきではありません。

対策 8

個人情報と権利侵害

ビッグデータという言葉が数年前から使われ始めています。簡単に言うと大容量のデータを高速に分析できるようになったことから、色々なデータを集め、事業活動に有効利用しましょうということです。例えば、オンラインショップでの利用者の行動履歴を解析し、お薦めの広告を出したり、SNS の情報を解析し、知り合いかもしれない人を表示したり、普段の位置情報を解析し、その人の勤務先や自宅の天気や渋滞情報を案内したりと、あなたの位置情報、Web サイトでの検索・入力・言語変換の履歴、エラーが発生した際の情報など、様々な情報が収集され、サービスやアプリケーションの向上に役立てられるようになりました。

また、情報、画像、音楽、映像などのコンテンツを容易に検索しアクセスできるようになりました。さらにコンテンツをブログ、SNS などを通じ、簡単に発信・共有できるようになりました。

このようにビッグデータの収集が活発化し、コンテンツの発信・共有が容易になった近年、どのようにインターネットと付き合えばよいのでしょうか。ここでは、あなたの個人情報が悪用されたりプライバシーの侵害に遭わないために、また、あなたが誰かの権利を侵害したり、不法行為をしないために、何に注意すべきかを解説します。

個人情報と権利侵害に関する 4つのポイント

8-1 パソコンやスマートフォンで収集される情報を確認する

8-2 Webサイト閲覧履歴などの共有範囲を確認する

8-3 SNSでの個人情報公開に注意する

8-4 知的財産や個人情報などの権利や法令を意識する

8-1 パソコンやスマートフォンで収集される情報を確認する

パソコンやスマートフォンなどで使う共通の Google アカウント、Apple ID、MS アカウントなどでは、利用履歴などの情報が活発に収集されており、利用者が提供したくないと感じる情報も収集されている可能性があります。Android、iOS、Windows 10 以降などでは、初期設定のまま提供者の推奨設定を選択すると様々な情報が収集の対象となります。プライバシー設定をよく確認し、自分が提供してよいと思える情報に限定するようにしましょう。

各 OS のプライバシー設定

■ **Windows 10**
［設定］›［プライバシー］

■ **macOS**
［システム環境設定］›［セキュリティとプライバシー］›［プライバシー］

■ **iOS**
［設定］›［プライバシー］

■ **Android**
［設定］›［Google］›［個人情報とプライバシー］
［設定］›［アプリ］›（各アプリを開く）›［許可］

8-2 Webサイト閲覧履歴などの共有範囲を確認する

Web ブラウザによる Web サイトの検索、閲覧、Web サービスの利用は、金銭管理に関わる情報、業務情報、個人の趣味趣向や思想など、利用者の業務やプライバシーにかかわる情報を多く含んでいます。

他の利用者と共有するパソコンにおいては、Web サイト閲覧などの履歴情報だけでなく、認証情報（ログイン中の状態）もパソコン上に残ることがあり、**他人に履歴情報を閲覧されるだけでなく、利用していた Web サービスなどにログインされてしまう危険性があります。こういった情報が残ることを防ぐため、共有するパソコンで、Web サービスを利用する際には、必ず Web ブラウザのプライベートブラウジングを利用しましょう**（Internet Explorer 11・Edge は InPrivate ブラウズ、Chrome はシークレットモード、Firefox はプ

ライベートウィンドウ、Safari はプライベートブラウズとそれぞれ名前が違います)。そのうえで利用後には、必ずログアウトし、Web ブラウザを終了するようにしましょう。

また、Edge と MS アカウント、Chrome と Google アカウント、Safari と Apple ID などクラウドサービスのアカウントと連携可能な Web ブラウザは、Web サイト閲覧履歴、ブックマーク、ID・パスワードなどをクラウド上に預けて（保存して)、どのデバイスからでも利用可能にしている一方、閲覧履歴などをビッグデータとして活用する場合もあります。Web ブラウザやクラウドサービスのアカウントのプライバシー設定をよく確認し、パソコン・スマートフォン・タブレットなどの機器より外に出したくない項目をオフに設定しましょう。

8-3 SNSでの個人情報公開に注意する

SNS の使い方やモラルについては、学生向けの「SNS 利用にあたって知ってもらいたい５つのこと」（SNS ガイドライン）が大変参考になりますので、一度は読んでおくようにしましょう。

SNS は、自分の個人情報が悪用されるという観点、さらに（あなたが投稿した情報や SNS のつながりなどで）あなたの友人の個人情報が悪用される可能性があるという点で注意が必要です。特にコメント、アップロードした写真などに写り込んだ背景など、複数の情報を組合わせて個人が特定される可能性があります。**１回の投稿では個人を特定することはできなくても、投稿を組合わせて個人が特定可能となるケースがあることに注意しましょう。**

また、意図せず（主に SNS やサービスへの規約や技術的理解不足から)、個人情報を公開してしまうケースも増加しています。

意図せず個人情報を公開してしまう例

- 公開範囲を確認せずに使っている
- 公開範囲を誤って設定している
- 写真や投稿に位置情報が含まれることに気づいていない
- あなたの投稿を共有した友人が再共有・公開する
- SNS 運営者が投稿内容などの情報を収集し、目的外利用や第三者提供することを確認していない

こういった情報を悪用して個人を特定し、標的型攻撃メールや詐欺をおこなうより巧妙化した手口が増加しています。このような巧妙化した手口を見破ることは難しいため、**SNS の機能、公開範囲、サービス利用規約やプライバシーポリシー（対策 9-2「個人情報の取扱いについて確認する」参照）などをよく確認し、意図しない個人情報の公開を避けましょう。**

参考：立命館大学　SNS 利用にあたって知ってもらいたい 5 つのこと、SNS ガイドライン
http://www.ritsumei.ac.jp/rs/sns/

参考：総務省　国民のための情報セキュリティサイト「SNS 利用上の注意点」
http://www.soumu.go.jp/main_sosiki/joho_tsusin/security/enduser/security02/05.html

参考：日経 BP　SNS の落とし穴：こんなはずじゃなかった！ SNS で個人情報がダダ漏れ、取り返しのつかないことに
http://www.nikkeibp.co.jp/article/matome/20131125/374827/

解説⑫

位置情報取得機能や画像に埋め込まれる位置情報

位置情報を取得可能な機器（携帯電話、スマートフォン、一部のデジタルカメラ）で写真を撮った場合、画像にはその写真を撮った位置情報が埋め込まれます（ジオタグと呼びます。下図は iPhone のカメラが埋めた情報を Windows 上で確認したもので、緯度・経度情報が表示されています。）。緯度・経度情報があれば、地図アプリなどで簡単に場所が判明します。

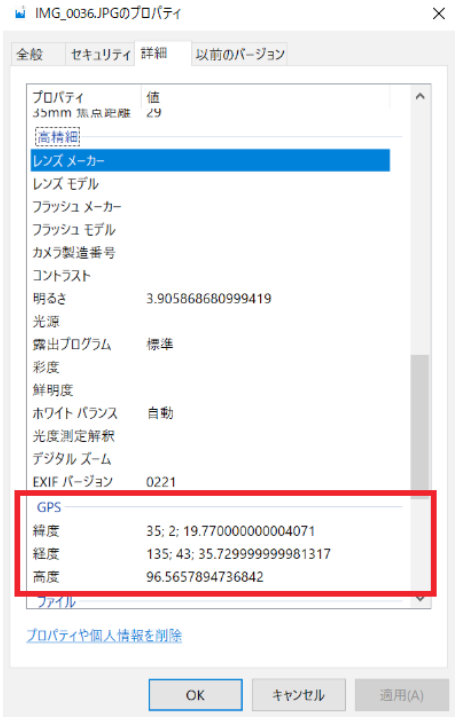


図 23　iPhone で撮影した写真のプロパティ

また、Twitter の SNS アプリなどでは、テキストの投稿なども位置情報公開につながるケースがあります。写真を撮影した場所や投稿した場所、投稿の内容を照らし合わせることで、それがどういった場所なのか（自宅など）判明することがあります。

＜事例「自宅で猫の写真を撮って投稿」＞

A さんは、SNS で本名を公開しています。ある日、A さんは自宅で猫をスマートフォンで写真を撮って、SNS で公開しましたところ、数日後から A さん宛に架空請求などの郵便が届くようになりました。

さらに行動解析などによって自宅や職場が推定されることがあります。SNS 利用では、特に位置情報に気を付けましょう。

Tips 10

秘密の質問と SNS

対策 4「メール」では、標的型攻撃メールや詐欺の下調べとして、利用者本人に関わる様々な情報が掲載される SNS が利用されるケースがあることを紹介しました。似たような考え方で「秘密の質問」と SNS で気をつけるべきことがあります。

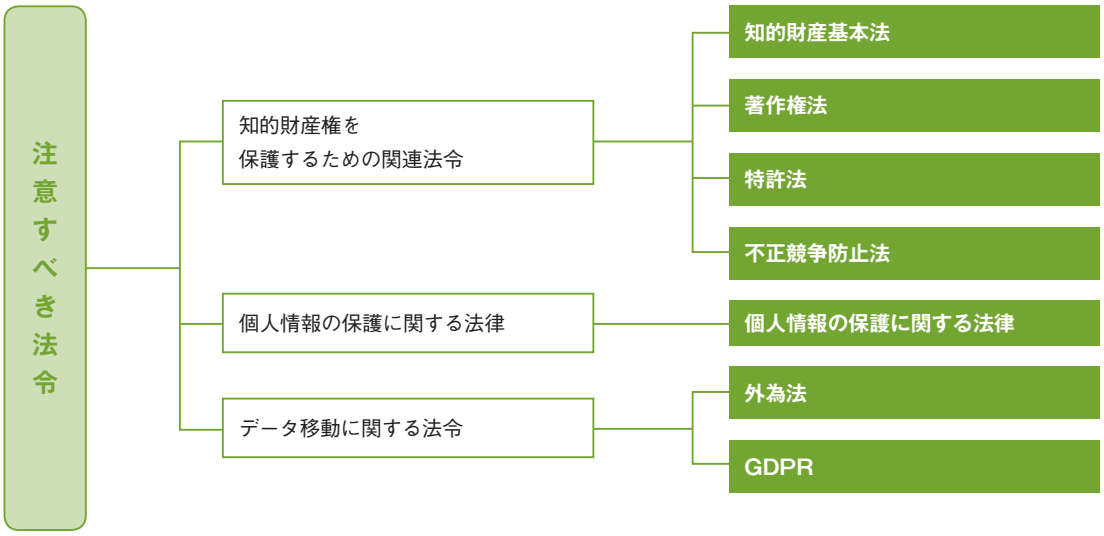
「秘密の質問」とは、パスワードを忘れた利用者が再発行や通知を受ける手続き時に、ユーザー登録時などに予め決めておいた本人しか知らない質問を入力することで本人確認をする機能です。「母の旧姓は？」「好きな食べ物は？」「ペットの名前は？」などの質問があります。この秘密の質問は、効果のある本人確認方法のように見えますが、正直に答えると非常に危険です。なぜなら、身近な人が知っている情報であったり、**SNS で様々なことを公開しているとより推測が容易になったり、秘密の質問の答えそのものを意識せずに公開している場合があるからです。**このように、容易に ID・パスワードを窃取される恐れがあることから、認証の仕組みとして「秘密の質問」を廃止する呼びかけが広まっています。

「秘密の質問」の答えを登録する場合には、推測される可能性のある正解を使わないようにしましょう。

参考 IPA「その秘密の質問の答えは第三者に推測されてしまうかもしれません」
https://www.ipa.go.jp/security/txt/2015/07outline.html

8-4 知的財産や個人情報などの権利や法令を意識する

インターネットを利用する上で意識すべき法令は、下図に示すような「知的財産権を保護するための関連法令」「個人情報の保護に関する法令」「データ移動に関する法令」の 3 つです。



引用元：図解入門ビジネス　最新 ISO27001 2013 の仕組みがよ～くわかる本

図 24　意識すべき法令

第一に「知的財産権を保護するための関連法令」についてです。インターネットが身近になったことで、画像、音楽、動画、文書などに代表されるコンテンツの入手、複製、公開、共有が非常に容易になりました。こういったコンテンツには、著作権に代表される知的財産権があり、法令により保護されています。著作権法では「学校教育の目的上必要と認められる限度において」「営利を目的としない」など、授業や教材への著作物の利用について寛容な部分はありますが、解釈が間違っていたり、使用許諾契約により利用範囲を制限されていたりするケースもあります。著作権だけではなく産業財産権（商標権、特許権、実用新案権、意匠権）、営業秘密など知的財産権全般についても配慮が必要です。例えば、本人承諾を取っていない誰かの顔が映り込んだ写真や映像をインターネットで公開または共有すれば、権利侵害となります。

第二に「個人情報の保護に関する法令」も多くの個人情報を扱う本学園にとって重要です。「学校法人立命館個人情報保護規程」（以下、個人情報保護規程）では、教職員には個人情報を適正に管理することが責務とされており、個人情報保護規程、個人情報の保護に関する法律（以下、個人情報保護法）およびガイドラインをよく理解した上で、教育研究活動・管理運営などの業務において、遵守するようにしましょう。

第三に「データ移動に関する法令」は見落としがちですが、注意してください。重要なものは、「外国為替及び外国貿易法」（以下、外為法）と「General Data Protection Regulation」

（EU 一般データ保護規則、以下、GDPR）の２つです。外為法は、安全保障輸出管理観点から、武器や軍事転用可能な技術が特定の地域に渡らないようにするためのもので、情報はインターネットを通じ、簡単に国境を超えるので注意が必要です。GDPR は日本の個人情報保護法と同様に、欧州経済領域（EEA 域内）における個人情報保護のための法律で、日本よりも厳格なルールとなっています。EEA 域内に所在する個人から越境して個人情報を取得するケース、および EEA 域内から個人情報を EEA 域外に越境するケースにおいて、GDPR の基準を満たす必要があるので注意が必要です。

さらに、法令には明記されていませんが、プライバシー権や肖像権も過去の判例に基づき憲法 13 条の幸福追求権や個人の尊重から人格権の一部として認められており、侵害すれば不法行為となります。情報（ここではデータやコンテンツ）によっては、秘密保持契約（NDR）や使用許諾契約などで法的に規制される場合もあります。

権利侵害や不法行為を起こさないために、まずは、**インターネットでデータやコンテンツを活用する際には、様々な制約・制限によって縛られるということを意識して、どの範囲で使ってよいのか、誰に見せてもよいのか、といった制限事項を把握しましょう。**

そして、**複製、公開、共有が容易なインターネットの世界において、前述の情報に課せられた制限事項に合わせた適切なアクセス権の設定（対策６「アクセス権の管理」参照）を実施する**ことで、誤ってインターネット公開したり、共有により情報が漏えいするような事態を避けましょう。

参考：一般社団法人 日本著作権教育研究会　著作権 Q & A
http://jcea.info/Q&A.html

参考：社団法人私立大学情報教育委員会「教員のための個人情報活用ガイドライン」
http://www.juce.jp/kojin_joho/
※ 2017 年度改正前のガイドラインです

参考：個人情報保護委員会
https://www.ppc.go.jp/

解説⑬

国境を越えてはいけない情報

情報が国境を越えることを規制する代表的な法令に「外為法」と「GDPR」があるのは前述の通りです。物理的なものであれば、それが国境を越えることはイメージしやすいのですが、インターネットの世界で情報を「持ち出してはいけない」「国境を越えてはいけない」という状況は少しイメージしにくいかもしれません。

例えば、「外為法」により規制対象となる情報を、誤ってインターネット公開する、特定地域からのアクセスを許可する、特定地域国籍を持った相手に共有した場合、**学内に設置したサーバーであっても規制対象となります**。逆にクラウドサービスなどでデータ保管場所（クラウドサービスのデータが実際にあるデータセンター等の場所）が特定地域にあったとしても、特定地域からのアクセスが規制されていれば、問題ありません。

一方、「GDPR」では、EEA 域内に所在する個人に関するあらゆる情報を域外の「十分性認定（十分なデータ保護レベルを確保していると EU が認定すること）」を受けていない第三国に移転することが制限されています。日本は 2018 年現在、この「十分性認定」を受けていないため、EEA 域内で収集した EEA 域内に所在する個人の情報を日本（学内や日本のデータセンターを使うクラウドサービス）に持ち込む場合や、EEA 域内を含む個人から情報を収集する場合には、GDPR の基準を確認し、対応する必要があります。しかし、Google、Amazon、Microsoft などの契約条項を提供するサービス上で情報を管理することは可能です。詳しくは各サービスの FAQ をよく読みましょう。

参考：立命館大学の安全保障輸出管理関連の資料・様式等
http://www.ritsumei.ac.jp/research/member/study_ethic/se15.html/

対策 9

サービス利用

インターネット上には消費者向け、組織向け（ビジネス向けや業務用途を想定したもの）など、様々なサービスがあります。また、個人運営、企業運営など、様々な提供者がいます。**利用者は、このサービス上でデータ（またはファイル）を作成･保存しています。提供者が管理するサービス上に利用者の所管するデータを保管しているわけですから、「提供者にあなたのもつ情報を預けている」ということになります。**別の言い方をするとインターネット上のサービスを業務で利用をするということは、業務委託と同等のことをしていると言えます。よって、あなたの個人情報、プライバシーにかかわる情報、機密性の高い情報を預けるにあたり、信頼できる企業が提供する、かつ信頼できるサービスを選択することが重要です。

次に、サービスに定められている利用規約や契約条項を確認しなければいけません。利用者が「サービス利用規約」や「プライバシーポリシー」などの約款に同意して利用を開始すると、無償であっても互いに法的な契約が取り交わされたことになります。約款を読み飛ばす人も多いと思いますが、預ける情報が重要な情報であれば、必ず確認するようにしてください。ここでは、特に確認すべき項目について、解説します。

情報を預けるサービスにおいては、情報漏えい、データ消失、サービスの終了などのリスクがゼロになることはありません。こういった情報事故やサービス終了のリスクが発生した際に、係争により賠償を受けることはできるかもしれませんが、情報事故をなかったことにできるわけではありません。事故は起こり得るものとして事前に備えておくことが重要です。

ここでは、利用者が情報を預けるようなインターネット上のサービスを利用するときに発生するリスクを紹介し、その対策を解説します。

サービス利用に関する 6 つのポイント

9-1 信頼できるサービスを選ぶ
9-2 個人情報の取扱いについて確認する
9-3 預けたデータの取扱いについて確認する
9-4 データの保管場所、準拠法、管轄裁判所を確認する
9-5 データ消失に備える
9-6 サービスの内容変更や終了に備える

9-1 信頼できるサービスを選ぶ

インターネット上のサービスで信頼できるかどうかは、対策 1-5「信頼できるソフトウェア以外をインストールしない」で述べた提供者の身元、利用者評価に加えて、認証・認定評価の 3 点で判断します。

提供者の身元として、組織の規模、財務状況、事業継続年数、国籍という点も重要です。サービス開始からの年数、過去の情報事故とその対応なども可能な範囲で確認してください。

利用者評価としては、利便性やサポートに関する評価はもちろんですが、サービス分野において一定のシェアをもつ、導入・活用事例などで大きな組織や有名な組織が多い、といった観点も確認しましょう。

特に、機密性の高い情報を預ける場合、そのサービスの提供組織の情報管理における取り組みや取得している認証・認定などを確認しましょう。認証・認定は当該の機関が監査した結果であるため、客観的に情報管理を適正にしている証明になります。ISO/IEC 27001、27002、27017、ISMS、CSA STAR 認証、ASP・SaaS の安全・信頼性に係る情報開示の認定などを取得している企業が望ましいでしょう。また、クレジット決済などを扱っている場

合は PCI DSS を取得している企業が評価できます。

利便性のみを評価するのではなく、預ける情報の機密性に応じて、こういった３つの観点を踏まえて信頼できるサービスを選びましょう。

9-2 個人情報の取扱いについて確認する

インターネット上のサービスは、利用前に約款による本人承諾を得るという手続きをとります。そのため、約款を必要最低限確認することが重要です。インターネットに限らず、個人情報はサービス提供を受けるために預けるものですが、確認せずに同意すると、「クレジットカードを作成したら､関連企業からの保険勧誘の電話やメールが増えた」というように、当該サービス以外での利用や第三者へ提供される場合があります。

個人情報、利用履歴などプライバシーにかかわる情報などの収集が活発化したことは、対策８「個人情報と権利侵害」で述べた通りです。収集した情報をどのような目的で利用するか、どのような範囲で活用するかについては、必ず約款に記載されています。まず、収集した情報の利用目的を確認しましょう。当該サービス以外に利用する旨の記載がないか、あるとしても許容できる内容かどうかを確認しましょう。

利用範囲には大きく分けて「当該サービス内」「サービス提供者内の他サービスまで」「第三者への提供（サービス提供者以外の他サービス）」などの範囲があります。あなたの情報がサービス提供者以外にマーケティング等で利用されるかどうか、またそれは許容できる内容かどうかを確認しましょう。

2014 年に T ポイントを運営するカルチュア・コンビニエンス・クラブ（CCC）は、T ポイント利用のために利用者（T 会員）が提供した個人情報を、T ポイント提携先に第三者提供するとプライバシーポリシーを改定し、話題になりました。

インターネット上のサービスには、個人情報の入力が溢れていますので、**利用範囲をよく確認し、個人情報やプライバシーにかかわる情報を預けてよいか判断した上で、サービスを**

選択しましょう。

9-3 預けたデータの取扱いについて確認する

クラウドサービス（メールやオンラインストレージなど）を利用してデータを預けることは、パソコン（機器内）に保存する場合とは違うということを意識しなければいけません。**特にスマートフォン向けのアプリは、意識せずインターネット上にデータを預けていることが多くあります。**インターネット上で記憶されるデータは、その記憶領域もサービスの一部なので、サービス提供者にデータを預けていることになります。**さらに預けたデータをサービス提供者が何らかの目的で利用する可能性があるということを意識しなければいけません。**無償のサービスを中心に、利用者が預けたデータを解析し、サービス改善や事業活動に活用されることが多くなっています。

機密性の高い情報を預ける際に、そのデータの所有者との権利関係がどうなっているかを確認しましょう。（対策 8-4「知的財産や個人情報など権利や法令を意識する」参照）

まず、**サービス利用規約やプライバシーポリシーなどの条項から、預けたデータの所有者は「利用者である」「提供者である」といった記載を探しましょう。**「提供者である」場合は、すべての権利を委譲してよい情報かどうか確認します。記載がない場合は、問合せて確認するか、利用しない方がよいでしょう。

また、所有者があなたであっても、サービス提供のためにデータを処理する、法的機関からの要請があれば提出するなどといった記載が必ずあります。また、提供者が何らかの権利を有する、当該のサービス提供以外を目的としてあなたの情報を提供者が利用する場合もあります（無償の消費者向けサービスにその傾向が強くあります）。

あなたが預けた情報を「誰が」「どのような場合に」閲覧・利用するのか必ず確認しましょう。

9-4 データの保管場所、準拠法、管轄裁判所を確認する

重要な情報の場合、自分の預けたデータがどこの国に置かれているかという点も確認しましょう。データの保管場所に応じて、その国の法律や文化に基づいた対応がなされるからです。そういうことも踏まえた上で、情報の重要性に合わせて、データの保管場所をよく確認するようにしましょう。

インターネット上のサービスのデータの保管場所を把握することで、データ移動に関する法令、国によって違う個人情報保護法の対応、行政機関・司法機関によるデータ監査など、預けた情報に起こり得ること、対応しなければならないことが明確になります。

インターネット上のサービスでは、利用者の情報もしくは利用者が所有する情報が漏えい・消失する事故が多く発生しています。これらは、サービスが不正アクセスを受けた、サービス側に設定・操作ミスがあった、提供者組織（または再委託先）に内部犯がいた、提供者組織内でマルウェア感染があった、大規模災害があった、といった様々な理由で発生します。

これは一般的なサービス提供や業務委託と同様、利用者の管理が及ばないところで起きる事故なので、前述の信頼できるサービスを選ぶことで、事故に遭う確率を減らすことしかできません。

提供者側で情報事故が起きると、残念ながら漏えいした情報を取り戻したり、消失したデータを復旧したりすることはできません。最終的には、サービス利用規約に記載された提供者の免責事項を踏まえ、受けた損害に対する賠償を係争により請求することになります。その際に、適用される法律と管轄裁判所が重要です。国外の法律準拠、かつ国外裁判所での係争になると不利になるため、可能な限り日本国法、国内裁判所と明示されたサービスを選択するようにしましょう。

9-5 データ消失に備える

システム障害や設定・操作ミス、不正アクセスなどによるデータ消失の危険性は常にあります。発生率に差はありますが、システムの世界では万が一の事態を想定する必要があります。2012 年にファーストサーバ株式会社が、提供するレンタルサーバーサービスの全データをバックアップ含めて消失するという事故を起こし、5500 件以上の顧客の Web サイトのデータ、メールデータなどが消失しました。過去には Gmail や Dropbox でも一部利用者のデータが消失する事故が発生しています。

インターネット上のサービスを利用する場合は、できるだけデータ消失が起こりにくいサービスを選ぶ、またデータ消失に備えて、自身でバックアップを取ることが必要です。

データ消失が起こりにくいサービスは、そのバックアップ方式（バックアップが何重になっているか、多拠点に保管されているか）などを確認すれば見つけることができます。また、重要なデータは、自身で手元にエクスポートしてバックアップする方法を検討し、インターネット上のサービスで消失しても、別のデータから復旧できるような工夫をしましょう。

9-6 サービスの内容変更や終了に備える

2016 年にモバイルアプリのサーバー側処理を提供するサービス Parse.com の利用停止が発表され、日本でもその影響が話題になりました。サービスは、提供者の倒産、買収による方針転換、情勢による陳腐化、人気の低迷などの理由で終了するリスクがあります。終了だけでなく、無償サービスが有償になる（有償範囲が変更になる）、サービス内容や規約などが変更になるといったリスクもあります。

サービス内容変更や終了というリスクは、常に利用者側が負うことになります。インターネット上のサービスで重要な業務を行う場合や機密性の高い情報を預ける場合は、リスクが小さくなるようにサービスを選ぶ、実際にそうなったときに備えた事前対策が必要です。

リスクを小さくするためには、対策 9-1「信頼できるサービスを選ぶ」で述べた通り、提

供元の経営状況、シェアなどを確認し、サービス継続性の高そうなものを選びましょう。

事前対策としては、まずサービス利用規約にサービス終了に関する条項があるので、何日前に告知する、どこで告知するなどの内容の記載を確認するようにしましょう。事前告知があるといっても、データ消失同様にバックアップを取ることは重要です。また、類似サービスへの移行方法、サービスに依存しない手段などを日ごろから探し、そのサービスにロックイン（囲い込み）されない努力をしましょう。

対策 10

その他

これまで様々な対策を解説してきましたが、これまでの分類にあてはまらないリスクとその対策について解説します。

その他に関する 2つのポイント

10-1 廃棄・譲渡時にデータを消去する

10-2 ファイル共有ソフトを使わない

10-1 廃棄・譲渡時にデータを消去する

パソコン・スマートフォン・タブレット、ストレージ機器、USB メモリ、SD カードなど、機器や可搬記憶媒体に機密性の高い情報を一度でも格納したのであれば、廃棄・譲渡時には注意が必要です。なぜなら **OS 上でファイルを「ゴミ箱を空にする」「削除する」「ディスクをフォーマットする」「工場出荷状態に戻す」などの操作は、多くの場合、データ（ファイル）本体を削除せず、データ（ファイル）の管理情報のみを破棄するため、専用のデータ復元ツールを使うとデータを復元できる可能性があります。**これにより、中古パソコンなどから情報漏えいする事故が発生します。

よって、機密性の高い情報を格納したことのある機器や可搬記憶媒体を廃棄する際には、以下のような手段でデータを復元できないようにしましょう。

パソコン、ストレージ機器

パソコンやストレージ機器は、取り外し可能なハードディスクや SSD などの記憶装置を内蔵しています。

（軽量ノートパソコン、小型パソコンなどで取り外せない場合は、後述のスマートフォン・タブレットを参照してください。）

1. 専用データ消去ツール

正常に動作するパソコンやストレージ機器の場合、専用データ消去ツールを使うのが簡単です。ストレージ機器や USB メモリメーカーなどが自社製品のデータ消去のため、無償で配布していることがあります。有償･無償含めて他にも様々なメーカーが提供していますので、探してみてください。

SSD に対応していないツールも多いので、機器の記憶装置の種類をよく確認して、対応しているものを選びましょう。

2. 暗号化

ハードディスクや SSD などが暗号化されている場合（対策 5-4「機密性の高いデータを暗号化する」参照）､取り外す前のパソコンがないとデータの暗号化を解除（復号）できないので、別々に捨てるという方法もあります。

また、暗号化済みのハードディスクや SSD のデータを削除（または初期化）して、暗号化を解除（復号）、再暗号化するとデータを復元することができなくなります。

3. 物理破壊

故障して動作しない場合、または廃棄する場合、物理破壊が有効な方法です。パソコンやストレージ機器からハードディスクや SSD を取り出してドリルなどで破壊します。破壊の際はケガに注意しましょう。

4. 廃棄・回収・買取業者

廃棄・回収・買取業者などではデータ消去を含めて有償対応するサービスがあります。費用は掛かりますが手間がかかりません。業者の評判などを確認して､信頼できる業者に依頼するようにしましょう｡データ消去証明書などを発行する業者もありますので、信頼性を量る目安にしましょう。廃棄･回収･買取前にデータ消去などのすべきことを Web サイトで紹介しているところもありますので、事前によく確認しましょう。

スマートフォン・タブレット

スマートフォン・タブレットの記憶装置は、組込みメモリカードが使われています。これらは、スマートフォンの基盤から取り外すことができないようになっています。docomo、au、Softbank などキャリアのスマートフォンを使っている場合、後述の 1 ～ 3 は各キャリアのショップで対応してくれます。

「おサイフケータイ」を使って電子マネーを利用している場合、機器を初期化しても IC チップにデータが残るので、事前に削除しましょう。一般的には、各電子マネーデータ移行の手続きをすれば、データは消えます。キャリアのスマートフォンであれば、データ移行後に IC チップの初期化対応もしてくれます。

1. 工場出荷状態に戻す（機器のリセット）

スマートフォンは、暗号化してから工場出荷状態に戻すことで、データの復元ができなくなります。iOS は標準で暗号化されていますが、Android や Windows 10 は利用者自身が暗号化する必要があります。暗号化されている状態で、工場出荷状態に戻します。

2. 物理破壊

組込みメモリカードの場合、基本的に機器から取り外すことができないので、機器ごとドリル等で破壊します。

3. 廃棄・回収・買取業者

キャリアのショップ以外で回収を依頼する場合は、パソコンやストレージ機器同様に、信頼できる業者を選びましょう。

可搬記憶媒体

最後に USB メモリ、SD カード、CD、DVD などの可搬記憶媒体です。

1. 専用データ消去ツール

USB メモリ、SD カードなどは、ハードディスクや SSD 同様に専用データ消去ツールがメーカーなどから提供されることが多いので、探してみましょう。

2. 物理破壊

利用可能なメディアシュレッダーがあれば、廃棄したい媒体に対応するかを確認の上、利用しましょう。SD カード、CD、DVD など比較的破壊しやすいものは、ニッパーなどを使って破壊することができます。破片が飛び散ることがあるので、破壊の際はケガに注意しましょう。

3. 廃棄・回収業者

USB メモリなど可搬記憶媒体もデータ消去・廃棄サービスを提供する業者がありますので、パソコンやストレージ機器同様に、信頼できる業者を選びましょう。

社団法人電子情報技術産業協会（JEITA）より、以下の利用者向けガイドラインが出ていますので、参考にしてください。

- 「パソコンの廃棄・譲渡時におけるハードディスク上のデータ消去に関する留意事項」
- 「ストレージ上のデータ消去に関するガイドライン」
- 「メモリカードの廃棄・譲渡時における内部のデータ消去に関するユーザ向けガイドライン」

10-2 ファイル共有ソフトを使わない

最近では随分と聞かなくなりましたが、2000 年頃の WinMX に始まり Winny や Share など P2P ファイル共有ソフト（もしくはファイル交換ソフト）という利用者同士がパソコン上にあるファイルを検索し、共有（交換）するアプリケーションがあります。

映画、TV 番組、音楽、書籍、ソフトウェアなどのうち著作権違反コンテンツ、いわゆる

「海賊版」を共有（交換）する利用者が後を絶たず、流行とともに問題視され、国内でも数十万人の利用者がいたとされています。

P2P ファイル共有ソフトの問題点は、第一に利用目的が「著作権違反コンテンツを入手するため」という利用者が多いことです。他人の著作物をインターネット上に公開し、第三者と共有することは犯罪です（対策 8-4「知的財産や個人情報など権利や法令を意識する」参照）。

第二に、P2P ファイル交換ソフトのネットワーク網を使い著作権違反コンテンツに見せかけたマルウェアを配布する攻撃者が多数存在するため、マルウェア感染のリスクが高いことです。

第三に、P2P ファイル共有ソフトの機能とネットワーク網を悪用した Antinny に代表されるマルウェアです。これに感染すると、パソコン内の様々なデータファイルを P2P ネットワーク網に意図せず共有（交換）されてしまいます。2004 年頃より情報漏えいの原因として注目されるようになり、2006 年には Winny を介したマルウェアによる情報漏えいが報告された後、政府をはじめとして P2P ファイル共有ソフトの利用を控えるよう注意喚起され、社会問題となりました。

これらの問題から Winny、Share、Perfect Dark、Cabos などのファイル共有ソフトは使ってはいけません。また、BitTorrent は、数 GB の大容量ファイルをダウンロードする際などに利用することがあるかもしれませんが、違法な目的での利用はしてはいけません。

参考：NetAgent 2015 年最新 P2P 利用状況調査
http://www.netagent.co.jp/product/p2p/report/201501/01.html

Chapter 3

第３章

情報事故が起きてしまったら

第２章「情報事故を起こさないための対策」では、予防策について解説してきました。しかし、サイバー攻撃は日々高度化・巧妙化していること、人的ミスは避けられないことなどから、交通事故と同様に情報事故の発生を完全に防ぐことはできません。よって、**情報事故は誰の身にも起こり得るものとして捉え、もしものときにどのような行動をとるべきかを事前に把握しておく**ことが重要です。

本章では、「情報事故が起きてしまった」ときの適切な対応について、想定される情報事故の種類ごとに解説します。

情報事故が起きたときの緊急連絡受付窓口

情報事故はネットワーク上で起こると急速に被害が拡大するため、どのような情報事故であっても「初動対応」において迅速に適切な対応を行う必要があります。また、事故発生原因や対応を一元的に把握し学園内で情報共有を行うことで、情報事故の再発防止につながります。

情報事故が起きてしまったら、後述の「情報事故の種類別の対応事例」を踏まえ適切な対応をとり、速やかに以下の「緊急連絡受付窓口」に報告・相談してください。

情報セキュリティ事故緊急連絡受付窓口

http://www.ritsumei.ac.jp/rainbow/security-contact-ritsumei/

※情報事故は誰の身にも起こりうるため、緊急連絡受付窓口に報告することで個人の責任が問われることはありません。

情報事故の種類別の対応事例

ここでは情報事故の種類別の適切な対応について解説します。より迅速な対応が求められるものには初動対応と記載しています。情報事故発生時は、初動対応後に情報セキュリティ事故緊急連絡受付窓口に連絡してください。

マルウェアに感染した場合の対応

マルウェアの感染は、利用者自身は気づかず、他者から指摘されて発見することが多い情報事故ですが、ランサムウェアのように、身代金要求のメッセージが表示されたり、ファイルがロックされたり直接的な被害で気が付くこともあります。マルウェア感染は被害拡大のスピードが速く影響の範囲も大きいため、下記の対応を迅速におこなってください。

対応

1 ネットワークから切り離す 初動対応

遠隔操作、オンラインバンクへの不正送金、外部へのサイバー攻撃、周辺の機器への拡散など、二次被害はネットワークを通じて広がります。そのため、被害を拡大させないために、有線の場合は LAN ケーブルを抜く、無線の場合は無線 LAN（Wi-Fi）の物理スイッチをオフ（ない場合は、OS の設定でオフ）にするなどして感染した機器をネットワークから切り離してください。

2 バックアップ

感染機器に格納されていた情報は、情報自体がマルウェアに感染している場合がありますので取り扱いには注意が必要です。やむをえずバックアップを行う場合は、外部メディアにバックアップしてください。

3 感染機器の復旧

感染した機器を再び利用する際は、OS のクリーンインストール、もしくは工場出荷状態に戻した上で使用してください。

ID・パスワードを窃取された場合の対応

ID・パスワードを窃取された結果、不正アクセスがあったとしても、多くの場合利用者は気づきませんが、サービスによっては、身に覚えのない変更通知メール、不正ログインの警告通知、ログイン履歴を確認できるものなどから、判明することがあります。他者が起こした情報事故により、利用者の ID・パスワードが漏えいした可能性があると連絡がある場合もあるかもしれません。

ID・パスワードが窃取された場合は、速やかに下記の対応をおこなってください。

対 応

1 パスワードを変更する 初動対応

被害を拡大させないために、パスワードを変更してください。

パスワードが変更されてしまってアクセスできない場合は、システム提供者（管理者）に連絡し、対応を依頼してください。

2 サービスの設定を確認する

ID・パスワードを窃取し不正にログインした攻撃者により、サービスの設定を悪意のあるものに変更されている場合がありますので、サービスの設定を確認してください。

本学の ID・パスワードが窃取された場合は、メールシステムなど本学の ID で利用しているサービスの設定を確認してください（メールシステムの場合、攻撃者のメールアドレスに転送されるなど、設定を変更されている可能性があります）。

モバイル端末や外部メディアの紛失、情報の誤送信・誤公開をした場合の対応

スマートフォン、ノートパソコンなどのモバイル端末を紛失し、悪意のある者に拾得された場合、モバイル端末内の個人情報を窃取されたり、ID・パスワードを記憶していたWebサイトに不正アクセスをされてしまう可能性があります。

USBや外付けHDDなどの記憶媒体を紛失した場合も、紛失した外部メディアに格納されていた情報が漏えいする危険性があります。

メールを誤送信してしまったり、オンラインストレージなどで共有範囲を間違って公開してしまった場合も情報漏えいにつながってしまいます。

このような「情報漏えい」の危険性がある情報事故に対しては、下記の対応をおこなってください。

対 応

1 （モバイル端末の場合）情報削除またはロック 初動対応

対策7-1「盗難・紛失時も情報にアクセスされない工夫をする」にて述べたリモートワイプ機能を設定していた場合は、速やかに実行しましょう。

また、紛失したモバイル端末がスマートフォンなど、通信契約を結んでいる端末の場合は、携帯キャリアに連絡をおこない、下記の対応ができないか相談してください。

- おおよその位置の検索
- 機器のロック
- 回線の一時停止

2 格納されている情報の確認

格納されている情報の機密性、それらが情報漏えいした場合の影響の範囲や度合いを明確にしてください。

3 情報事故発生の報告

個人情報等の機密性の高い情報が格納されていた場合は、その情報の関係者（教職員については所属長）に速やかに報告してください。

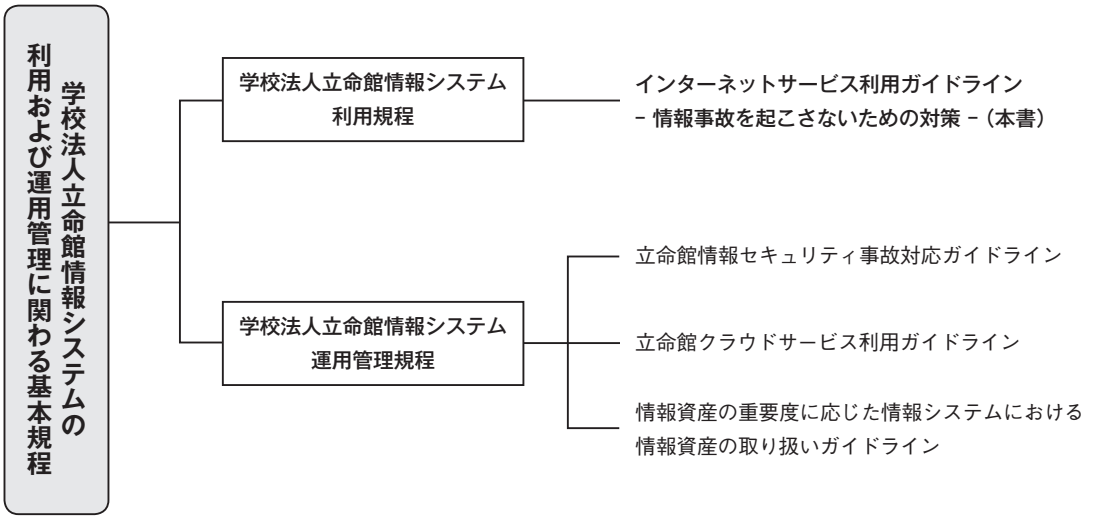
情報システムを運用管理されている方へ（ガイドライン）

本学では、情報システムの運用管理者を対象に、情報セキュリティ事故対応の具体的な対策指針や注意事項をまとめた**「学校法人立命館情報セキュリティ事故対応ガイドライン」**を策定していますので、情報システムを運営する方はガイドラインを必ず確認してください。

付録 A 関連規程

情報環境を利用する際には本ガイドライン以外にも気を付けるべき規程やガイドラインがあります。**教職員の方は以下の規程、ガイドラインを必ず確認してください。**

情報セキュリティ関連の規程・ガイドライン



リスクマネジメント基本要綱

情報管理・セキュリティ事故が発生した場合、リスクマネジメント委員会に指定の書式で報告します。

学校法人立命館個人情報保護規程

第 16 条に「個人情報の取り扱いについて、本規程に抵触する事実があると判断した場合は、その事実について速やかに調査し、個人情報学校管理責任者に報告しなければならない。」と定められています。また、事務局（課・事務室）には、これに合わせて総務課への電話連絡、指定の書式「個人情報保護事案報告シート」の提出が義務付けられています。

参考資料

IPA（独立行政法人　情報推進化機構）

情報セキュリティ読本（書籍）
ISBN978-4-407-33076-2

対策のしおりシリーズ（配布 PDF）
http://www.ipa.go.jp/security/antivirus/shiori.html

IPA テクニカルウォッチ
標的型攻撃メールの傾向と事例分析＜ 2013 年＞
～ますます巧妙化、高度化する国内組織への標的型攻撃メールの手口～

IPA テクニカルウォッチ
標的型攻撃メールの例と見分け方

NISC（内閣サイバーセキュリティセンター）

ネットワークビギナーのための情報セキュリティハンドブック（Ver.2.11）
http://www.nisc.go.jp/security-site/handbook/

総務省

国民のための情報セキュリティサイト
http://www.soumu.go.jp/main_sosiki/joho_tsusin/security/

フィッシング対策協議会

利用者向けフィッシング詐欺対策ガイドライン（2016 年度版）
https://www.antiphishing.jp/report/guideline/

LAC（株式会社ラック）

Cyber GRID View vol.1
日本における標的型サイバー攻撃の事故実態調査レポート
https://www.lac.co.jp/lacwatch/report/20141216_000198.html

JNSA（NPO 日本ネットワークセキュリティ協会）

JNSA 2014 年 情報セキュリティインシデントに関する調査報告書
JNSA 2015 年 情報セキュリティインシデントに関する調査報告書
JNSA 2016 年 情報セキュリティインシデントに関する調査報告書
http://www.jnsa.org/result/incident/

図解入門ビジネス 最新 ISO27001 2013 の仕組みがよ～くわかる本

打川和男 著　株式会社秀和システム
ISBN978-4-7980-3982-4

徹底攻略 情報セキュリティマネジメント教科書　平成 28 年度

著者　株式会社わくわくスタディワールド　瀬戸美月／齋藤健一
株式会社インプレス
ISBN978-4-8443-3987-8

INDEX 索引

GDPR …… 84
HTTP 通信 …… 57
HTTPS 通信 …… 57
OS …… 16
S/MIME …… 50
SNS …… 79
VPN …… 61
Web …… 32
Web サービス …… 32
Web サイト …… 32
Web ブラウザ …… 32
Web ページ …… 32

あ行

アカウントリスト攻撃 …… 26
アクセス権 …… 65、69、71
アップデート …… 16
アドバタイジング攻撃 …… 34
アプリケーションソフトウェア …… 19
暗号化 …… 56、59、63
エクスプロイトツール（キット） …… 34
オンラインストレージ …… 67

か行

外為法 …… 84
拡張子 …… 43
キーロガー …… 21
強度 …… 24
グリーンバー …… 36
個人情報 …… 77

さ行

再共有 …… 67
辞書攻撃 …… 25
情報セキュリティ対策 …… 8
ショルダーハッキング …… 24
脆弱性 …… 16
セキュリティ対策ソフト …… 14
ゼロディ攻撃 …… 21
送信ドメイン認証 …… 53
ソーシャルエンジニアリング …… 24
ソーシャルログイン …… 29

た行

多要素認証 …… 30
知的財産権 …… 82
デジタル証明書 …… 50、57
電子署名 …… 50
トラッシング …… 24

は行

パスワード管理ツール …… 27
ビッグデータ …… 77
秘密の質問 …… 82
標的型攻撃メール …… 47
標的型サイバー攻撃 …… 47
ファームウェア …… 18
ファイル共有ソフト …… 96
ファイル転送サービス …… 55
フィッシング …… 44
プライバシー設定 …… 78
プライベートブラウジング …… 78
ブルートフォース攻撃 …… 25

ま行

マルウェア …… 14
迷惑メール …… 40
モバイル端末（デバイス） …… 73

ら行

ランサムウェア …… 22
リモートワイプ機能 …… 74
ログイン履歴 …… 30
ロックイン …… 92

わ行

ワンクリック詐欺 …… 37

インターネットサービス利用ガイドライン

発　行　日　2019年4月1日
編　　集　立命館情報基盤整備委員会
発　　行　学校法人 立命館
〒604-8520　京都市中京区西ノ京朱雀町1
印刷・製本　株式会社　石田大成社