# 情報セキュリティ対策の基本
# と
# 共通対策

情報セキュリティ 10 大脅威 2023 版


独立行政法人情報処理推進機構
セキュリティセンター

2023 年 2 月

### ①情報セキュリティ対策の基本

世の中には「情報セキュリティ 10 大脅威」へランクインした脅威以外にも多数の脅威が存在する。とは言え、攻撃者が利用する「攻撃の糸口」は似通っており、脆弱性を悪用する、ウイルスを使う、ソーシャルエンジニアリングを使う等の古くから知られている手口が使われている。

詳しくは「情報セキュリティ 10 大脅威 2015」[1] の 1 章で解説しているが、表 1.1 に示すように「攻撃の糸口」を 5 つに分類し、それぞれに該当する対策を「情報セキュリティ対策の基本」としている。「攻撃の糸口」に変化がない限り、「情報セキュリティ対策の基本」による効果が期待できるので、これを意識して継続的に対策を行うことで、被害に遭うリスクを低減できると考える。

**表 1.1** 情報セキュリティ対策の基本

| 攻撃の糸口 | 情報セキュリティ対策の基本 | 目的 |
|---|---|---|
| ソフトウェアの脆弱性 | ソフトウェアの更新 | 脆弱性を解消し攻撃によるリスクを低減する |
| ウイルス感染 | セキュリティソフトの利用 | 攻撃をブロックする |
| パスワード窃取 | パスワードの管理・認証の強化<br>※「共通対策」で詳細を解説 | パスワード窃取によるリスクを低減する |
| 設定不備 | 設定の見直し | 誤った設定を攻撃に利用されないようにする |
| 誘導（罠にはめる） | 脅威・手口を知る | 手口から重要視すべき対策を理解する |

また、昨今はクラウドサービスの利用も一般的になってきている。クラウドサービスを利用する場合は、表 1.2 の対策を「情報セキュリティ対策の基本」+ α として行うことで、被害に遭う可能性を低減できると考えるので参考にしてほしい。

**表 1.2** 情報セキュリティ対策の基本+ α

| 備える対象 | 情報セキュリティ対策の基本<br>＋ α | 目的 |
|---|---|---|
| インシデント全般 | 責任範囲の明確化（理解） | クラウドサービスを契約する際に、インシデント発生時は誰（どの組織）が対応する責任があるのかを明確化（理解）する |
| クラウドの停止 | 代替案の準備 | 業務が停止しないように代替策を準備する |
| クラウドの仕様変更 | 設定の見直し | 更新情報を定期的に確認し、仕様変更により意図せず変更された設定を適切な設定に直す（設定不備による情報漏えいや攻撃への悪用を防止する。） |

**参考資料**

1. 情報セキュリティ 10 大脅威 2015 (IPA)
https://www.ipa.go.jp/security/vuln/10threats2015.html

### ②共通対策

脅威の種類は多岐に渡るが対策に着目すると、共通しているものもある。このような対策は、複数の脅威に対して同時に行えるため効率的に対策を進めることができる。そこで、本項では表 1.3 の 7 つの対策について、「複数の脅威に有効な対策」として、注意事項、検討事項等も含めて具体的に解説する。

本項を読み、自身や自組織のセキュリティ対策を進めるうえで参考としてほしい。

**表 1.3** 複数の脅威に有効な対策集

| 対策 | 対象 | |
|---|---|---|
| | 個人 | 組織 |
| パスワードを適切に運用する | ○ | ○ |
| 情報リテラシー、モラルを向上させる | ○ | ○ |
| メールの添付ファイル開封や、<br>メールや SMS のリンク、URL のクリックを<br>安易にしない | ○ | ○ |
| 適切な報告/連絡/相談を行う | ○ | ○ |
| インシデント体制を整備し、対応を行う | | ○ |
| サーバーやクライアント、ネットワークに<br>適切なセキュリティ対策を行う | | ○ |
| 適切なバックアップ運用を行う | ○ | ○ |

## ■パスワードを適切に運用する[1]

個人や組織に関わらずパスワードの設定はオンラインショッピングやネットワークカメラ（見守りカメラ）等の様々な場面で必要になる。安易な設定や不適切な扱いをすると、攻撃者に不正ログインされやすくなってしまう。それでは適切な設定や運用とは具体的には何か？本項を読み、適切な対策を実施することでリスク低減の参考にしてほしい。

- 適切な設定をする[1]

・初期設定のままにしない

ネットワークカメラ等の IoT 機器では初期設定のパスワードは共通して使われている場合もあり、危険性が高いため変更する。

・推測されにくいパスワードを設定する[2]

推測されにくくするためには長く複雑にする事が有効である。内閣サイバーセキュリティセンターが発行しているインターネットの安全・安心ハンドブック[3]では、大文字と小文字のアルファベット、数字、記号を含んだ 10 桁以上を推奨している。パスワード作成は特に以下を意識するとよい。

①数字、アルファベット、記号等の複数の文字種を組み合わせる

②生年月日や名前を使わない

③連続した数字やアルファベットにしない

④単純な単語一語だけにしない

表 1.4　悪いパスワードの例

| パスワード | 悪い点 |
|---|---|
| 123456 | 連続した数字 |
| Password<br>p@ssw0rd | 単純な単語や<br>その類似系 |
| taro1202 | 名前や誕生日 |
| 1qaz2wsx | キーボードの縦配列 |
| qwerty | キーボードの横配列 |

・パスワードは使い回さない

個人情報や金銭情報を登録しているサービスや ID が登録したメールアドレスになるサービスでは特にパスワードの使い回しを避けた方がよい。複数のサービスで同じパスワードを利用していると、どこかで漏れた時に軒並み不正ログインされてしまう。また、使い回しを避けるためのパスワード作成方法を IPA で紹介しているのでパスワード設定時は参考にするとよい。[4]

- 適切な保管、運用を行う

・パスワードは他人に教えない

・ID とパスワードをセットで保管しない

例えば ID とパスワードのメモを端末に貼り付けていると、紛失した際に簡単に不正ログインされてしまう。どうしても覚えきれない場合は自宅で保管するノートに記録したり、パスワード管理ソフトを利用したりするとよい。

・スマホや PC にパスワードのメモを貼らない

・複数人で使用する端末ではブラウザにパスワードを記憶させない

便利な機能だが複数人で利用している端末では、自分以外の人が自分になりすましてログインできてしまうので注意が必要である。

- 不正ログインされてしまった時の対応

・パスワードを変更する

今後の不正ログインを防ぐために即時パスワードを変更する。

・パスワードを使い回していないか確認する

他のサービスでパスワードを使い回しているのであれば合わせてパスワードを変更する。

**参考資料**


1. 不正ログイン対策特集ページ(IPA)
https://www.ipa.go.jp/security/anshin/account_security.html
2. チョコっとプラスパスワード（IPA）
https://www.ipa.go.jp/chocotto/pw.html
3. インターネットの安全・安心ハンドブック(内閣サイバーセキュリティセンター)
https://security-portal.nisc.go.jp/guidance/handbook.html
4. 安心相談窓口だより
「不正ログイン被害の原因となるパスワードの使い回しは NG」(IPA)
https://www.ipa.go.jp/security/anshin/mgdayori20160803.html

## ■情報リテラシー、モラルを向上させる

意図せず情報モラルに反する事を行ったり、故意に不正を行ったりする人がいる。組織においては業務で急いでいたり、緊急対応をしていたり等、精神的に追い込まれて、組織のためによかれと考えてルールに反してしまうこともあると考える。いずれにしても、悪気があるかないかに関わらず自身の行為には責任が伴う。特に、組織においてはたとえ従業員の勝手な行動であったとしても組織への影響や責任が問われることが多くある。本項を読み、「個人として」、「組織として」どのように対策すべきかの参考にしてほしい。

● 家族や組織従業員を教育する

情報リテラシーの向上が必要な者は気を付けるべき事に自身で気付けないことが多い。個人であれば、これから PC やスマホを使う子へ、使い慣れていない親へ、組織であれば従業員への教育を行う。教育内容は教育対象とするケースにより異なるため一例として以下に記載する。

【個人、組織共通】

①SNS の利用に関するケース

・掲載されている情報が正しいとは限らない

悪意の有無に関わらず、誤った情報が広まるおそれもあるため、情報を鵜呑みにしない。

・安易に情報を拡散しない

情報を安易に拡散してしまうと責任を問われることがある。特に SNS では簡単に情報を見つけ、拡散できるが、意図せずデマの拡散や誹謗・中傷に加担してしまうおそれがある。

・情報発信は慎重に行う

真偽を判断できない情報や他人を攻撃するような発言は控える。一度インターネット上に発信した内容は完全に消去することは難しい。(デジタルタトゥーと呼ぶ)そのため、感情のままに発信せず、一旦時間をおいて落ち着いて行う。

②インターネット利用に関するケース

・本物に似せた偽のウェブサイトがある

・個人情報を盗もうとするウェブサイトがある

特に個人情報や金銭に関する情報の入力を求められた時には注意が必要である。

【組織】

①組織の情報セキュリティに関するケース

・情報リテラシーや情報モラルの向上を図る。

②組織のコンプライアンスに関するケース

・内部不正に対する懲戒処分やそれを規定した就業規則に関する周知を行う。

教育のコンテンツに何を取り入れるべきか業務により異なるが IPA から発信しているコンテンツを紹介するので参考にしてほしい。[1,2,3,4]

③教育受講時の心得

教育する際は受講者に以下のことを意識づけすることも必要である。

・他人事と考えずに受講すること

・就業規則、社内運用ルールを理解すること

・事故を起こさない事は自分を守る意味もあること

・緊急時の報告先、報告方法を把握すること

● 継続的に取り組む

・定期的に、適切な時期に教育する

組織における教育では、人の入れ替わり(新入社員、派遣、出向等)やイベント(長期休暇、社会情勢等)を考慮することも有効である。

また、毎回同じ教育コンテンツではなく運用状況を確認し、コンテンツを見直すことも必要である。

**参考資料**

【個人、組織共通】

1. 情報セキュリティ啓発(IPA)
https://www.ipa.go.jp/security/keihatsu/features.html

【個人】

2. サイバーセキュリティのひみつ(IPA)
https://www.ipa.go.jp/security/keihatsu/security-himitsu/

【組織】

3. 対策のしおり(IPA)
https://www.ipa.go.jp/security/antivirus/shiori.html
4. 講習能力養成セミナー(IPA)
https://www.ipa.go.jp/security/keihatsu/sme/seminar.html

## ■メールの添付ファイル開封や、メールや SMS のリンク、URL のクリックを安易にしない[1]

様々なサービスからの連絡がメールで行われたり、SMS でお知らせが届けられたりすることがある。本物の連絡である場合もあるが、本物を騙った偽の連絡であるとそれを起因として個人情報を盗まれたり、金銭被害に繋がったりするおそれがある。

● 被害にあうタイミング

悪意があるメールや SMS を受信して、内容を閲覧した時点ではまだ情報を盗まれたり、端末がウイルス感染したりすることはない。そのメールや SMS から誘導されたウェブサイトに情報を入力することで入力した情報が盗まれ、添付ファイルを開くことでウイルス感染してしまう。

ウイルスに感染すると端末に保存されている情報が盗まれたり、端末が正常に動作しなくなったりしてしまう。

さらに盗まれた情報がクレジットカードや銀行口座の情報であるとそれを利用されて金銭被害につながってしまう。

● メールや SMS、SNS に関する注意事項

・安易にリンクや QR コードを開かない

悪意があるメールや SMS、SNS で受信したメッセージ内のリンクをクリックやタップして開く、または URL をブラウザに入力して開いたウェブサイトは正規のウェブサイトを模倣した偽のウェブサイトであるおそれがある。

・記載された電話番号に電話をかけない

悪意があるメールや SMS に記載された電話番号は偽のサポート窓口につながるおそれがあり、嘘の案内をされることで情報を聞き出されてしまう等の被害につながる。

● メール固有の注意事項

・画像をクリックやタップしない

一見ただの画像であってもリンクになっていて、クリックやタップをすると偽のウェブサイトが開かれるおそれがあるので注意する。

・添付ファイルを開かない

添付ファイルを開くと悪意のあるプログラムが起動し、ウイルス感染するおそれがある。

さらに、万が一 Microsoft Word や Excel を開いてしまった際は「コンテンツの有効化」というボタンが表示されることがある。このボタンを押すと悪意のあるプログラムが動いてしまうことがあるため、安易にクリックやタップをしてはいけない。

● リンクや URL をクリックせずに確認する方法

不審なメールや SMS の案内は以下のような、リンクや URL をクリックさせる文面が多い。

「〇〇について下記よりご確認下さい。」

「詳細はコチラ」

このような文面であるため、クリックやタップをしてはいけないとはいえ内容が気になる、確認はした方がよいと感じることがある。

その場合はメール内のリンクを疑い以下のようにして確認するとよい。

①ウェブページを検索して開き、確認する

対象のサービスをブラウザで検索して正規のウェブページを開く。そして、例えば不在通知ならば追跡番号で調べるか問合せをする。ショッピングサイトならばログインしてアカウント情報を確認したり、注文履歴を確認したり、問い合わせることで確認する。

②あらかじめブックマーク（お気に入り）しておく

よく利用しているウェブサイトはブックマークしておき、ブックマークからアクセスする。

③あらかじめ正規のアプリをインストールしておき、そのアプリを使ってサービスを参照する。

IPA では実際の画面を用いて紹介しているので、是非以下のウェブページで手口を確認し、不審なメールや SMS に備えてほしい。

**参考資料**

1. 安心相談窓口だより
「URL リンクへのアクセスに注意！」(IPA)
https://www.ipa.go.jp/security/anshin/mgdayori20210831.html

## ■適切な報告/連絡/相談を行う

【個人】

被害を受けた時は適切な人や機関への相談が必要である。誰にも相談せずに 1 人で対応してしまうとさらなる被害につながってしまうおそれもある。不安に感じた時や被害に遭った時は慌てず、まずは落ち着いて、以下を参考に誰かに相談してほしい。

表 1.5【個人】に関する相談先の例

| 発生した出来事 | 相談する相手 |
|---|---|
| 不審なメールや SMS を受信した<br>不審なウェブサイトを見つけた<br>不審なウェブサイトに個人情報や金銭情報を入力してしまった | ①信頼できる知人<br>②日本データ通信協会（迷惑メール相談センター）<br>(https://www.dekyo.or.jp/soudan/index.html)<br>③サービス提供会社<br>※不審なメールや SMS のリンクはクリックせず、不審なウェブサイトからではなく、自身でサービス提供会社の窓口を調べて問い合わせる<br>④クレジットカード会社や金融機関（情報を入力してしまった場合）<br>⑤フィッシング 110 番 (https://www.npa.go.jp/cyber/policy/phishing/phishing110.htm)<br>⑥フィッシング対策協議会 (https://www.antiphishing.jp/registration.html) |
| メールや SMS で脅迫された、金銭の要求をされた | ①信頼できる知人<br>②警察 |
| クレジットカードを勝手に使われた<br>インターネットバンキングで不正送金された<br>※③以下に連絡<br>電子決済を勝手に使われた | ①クレジットカード会社、電子決済の提供会社<br>※クレジットカード会社によっては、全額または一部を補償する場合がある。（補償してくれる期間が短い場合があるので注意）<br>②勝手に使われたサービスや商品の提供会社<br>③金融機関<br>④警察 |
| PC やスマホに不審な警告が表示された | 基本的には表示に従ってはいけないが心配な場合は以下に相談する。<br>①信頼できる知人<br>②IPA（安心相談窓口） (https://www.ipa.go.jp/security/anshin/) |
| 自分のアカウントに勝手にログインされた | ①ログインされたサービスの提供会社 |
| 誹謗・中傷を受けた | ①#NoHeartNoSNS（ハートがなけりゃ SNS じゃない！）（総務省総合通信基盤局）<br>(https://www.soumu.go.jp/main_sosiki/joho_tsusin/kyouiku_joho-ka/no-heart-no-sns.html)<br>②誹謗・中傷が掲載されているウェブサイトや SNS の提供会社<br>③警察や弁護士 |
| 上記のどれに当てはまるかわからない | ①IPA（安心相談窓口） (https://www.ipa.go.jp/security/anshin/)<br>②国民生活センター / 消費生活センター (https://www.kokusen.go.jp/map/) |

【組織】

組織においては適切に報告や連絡をしないと被害の拡大につながるだけでなく隠蔽したとされ、さらなる信頼の失墜につながるおそれもある。それを防ぐためにあらかじめエスカレーション先を定めて対応マニュアルを作成し、これに従ってエスカレーションを行う必要がある。また、場合によっては組織外への情報発信もしなければならない。これら一連のエスカレーションを迅速に行うために、組織に所属する全員がインシデント発生時の対応を十分に理解すること、経営者や上司、責任者は部下や担当者が包み隠さず躊躇なくエスカレーションできる風土や関係性を築くことも重要である。

対応マニュアルの作成においては、連絡先の例を以下に列挙するので参考にしてほしい。

表 1.6【組織】に関する報告・連絡・相談先の例

| 組織内の立場 | 報告・連絡・相談する相手 |
|---|---|
| 従業員 | 些細なことから重大インシデントを発見できる可能性がある。また、自身がインシデントを起こしてしまった場合は適切にエスカレーションをしないと隠蔽を疑われ、責任を問われるおそれがある。<br>そのため、躊躇せずにエスカレーションすることが重要である。<br><br>①上司やセキュリティの管理者にエスカレーションする<br>※自身がインシデントを起こした、発見した場合<br>②システム管理者にエスカレーションする<br>※自身が利用している端末やシステムに関するインシデントの場合<br>③CSIRT にエスカレーションする<br>※組織内で CSIRT が構築されている場合 |
| 上司や責任者 | 従業員としての対応だけでなく、報告を受け、対応を判断する必要もある。日頃から関係者を把握しておくことや対応手順を理解しておくことが重要である。<br><br>①組織内の関連部署へ横展開する<br>②組織外への情報発信を検討、判断する |
| 経営者や組織として | 場合によって、被害拡大防止や原因と対応の報告等を 1 次報告、2 次報告と段階を分けて適切に行うことが重要である。<br><br>①セキュリティの専門会社に技術支援依頼をする（契約がなくても、スポットで緊急対応してくれるサービスもある）<br>※自組織だけでは調査や解決できない場合<br>②顧客、取引先、委託先、委託元、関連組織に報告する<br>※場合によってはメディアへの公表を検討する<br>③金融機関、クレジットカード会社へ連絡する<br>※情報漏えい等によるさらなる被害拡大防止<br>④警察へ被害届を提出する<br>⑤監督省庁、IPA、JPCERT/CC、個人情報保護委員会に報告する<br>※発生したインシデントに併せて公的機関等に報告する<br>⑥弁護士に相談する |

## ■インシデント体制を整備し、対応を行う

セキュリティインシデントが発生した際、誰がどのように、何から行えばよいのか？これを理解してあらかじめ対応する仕組みを整えているのといないのとでは同じ事象の問題が起きたとしても受ける被害の大きさは全く異なる物になる。特に、サイバー攻撃を受けた際はより迅速な対応が必要になってきている。そこで、本項ではセキュリティインシデント発生時の対応やそれを行うために必要なことを解説するので、自組織における対策準備の参考としてほしい。

● インシデント対応の事前準備

・CISO（Chief Information Security Officer）等、専門知識をもつ責任者を配置する

・CSIRT（Computer Security Incident Response Team）を構築する

インシデント対応は一般社員が兼務して対応するのは難しい。そのため組織内の情報セキュリティ問題を専門に扱う CSIRT の構築が望ましい。構築するのが厳しい場合はインシデント対応の統制をする責任者を決めておく。

・CSIRT を中心とした有事の際の連絡先や対応フローを確立し、運用手順を作成する

・作成した運用手順を社員へ周知する

・実際に運用できるか確認する(訓練する)

作成した運用手順は、実際に運用できるのか定期的に訓練を行い、その結果を元に手順を見直すことも必要である。

・自組織で解決できない場合を想定して外部の協力依頼先を用意する

・これら全てを継続的に行える体制と社内ルールやポリシーの整備、予算の確保を行う

● インシデント対応として CSIRT が行うべき事

①検知/連絡受付

セキュリティ機器での検知や組織の外部や組織内の人間からの通報によりインシデントの発生を認知する。

②トリアージ

認知したインシデントについて通報者やインシデントに関係する可能性がある者とやり取りし、情報を収集することで事実確認をする。その後、確認した結果から CSIRT で対応すべきかどうかを判断する。判断した結果は通報者や関係者に連絡する。その際、対応すべきかどうかに関わらず速やかな対応が必要な場合や情報共有をすべき場合は注意喚起や情報発信を行う。

③インシデントレスポンス

インシデントの事象を分析し、対応計画を策定する。組織内の関連部門だけでは対応しきれない場合は外注先への技術支援依頼も視野に入れて、経営者等の責任者と連携して計画を立てることも必要である。技術的なこと以外でも外部の専門機関や関係する組織に支援依頼をしたり、情報を提供してもらったりする。

その後、策定した計画に従って対応を推進し、問題が解決しているかの確認をする。

④報告/情報公開

対応計画の策定や実施と並行してインシデントの通報者や関係者、メディアや社会、監督官庁への報告を行う。

CSIRT の構築が難しい組織であっても最低限インシデント対応を取り纏める者を定めておく必要がある。インシデント発生時に対応すべきことは公的機関が様々なガイドライン等を公開している。自組織では対応の準備ができているか事前に確認しておくことを推奨する。[1,2,3,4]

**参考資料**


1. サイバーセキュリティ経営ガイドラインと支援ツール（経済産業省）
https://www.meti.go.jp/policy/netsecurity/mng_guide.html
2. インシデント発生時に組織内で整理しておくべき事項（経済産業省）
https://www.meti.go.jp/policy/netsecurity/downloadfiles/CSM_Guideline_app_C.xlsx
3. CSIRT マテリアル 運用フェーズ（一般社団法人 JPCERT コーディネーションセンター）
https://www.jpcert.or.jp/csirt_material/operation_phase.html
4. サイバーインシデント緊急対応企業一覧（特定非営利活動法人日本ネットワークセキュリティ協会）
https://www.jnsa.org/emergency_response/

## ■サーバーやクライアント、ネットワークに適切なセキュリティ対策を行う [1.2]

組織に対する脅威はサーバーやクライアント、ネットワークが関連したものが多い。これらには重要な情報が含まれており、企業活動の生命線であることは今後も変わらないと考えられる。つまり、攻撃者からは今後も狙われやすいということである。個人の PC やスマートフォンとは異なり、組織のサーバーは「更新プログラム適用」1 つを見ても組織としてのポリシーの制定や要員確保、事前検証、手順の確立、そしてそれを維持し続ける予算の確保と仕組みが必要であり検討事項は多く、頭を抱える組織も多いと考える。本項ではサーバーやネットワークに対するセキュリティ対策の検討事項をまとめるので今後の運用の参考としてほしい。

- 脆弱性対策を適切に行う

・サポート切れの OS やソフトウェア、ハードウェアを使用しない

・迅速に更新プログラムの適用をする

漏れなく適用するために資産管理や脆弱性情報の収集、更新プログラムの適用状況を管理する手順や体制を整備しておく必要がある。

また、どのように動作検証を行うか、構築時や保守契約時に考慮しておく必要がある。

・仮想パッチを導入する

仮想パッチとは、直接的にソフトウェアの脆弱性を解決せずに、ネットワークレベルで攻撃の通信を遮断することである。サーバーに更新プログラムを適用するには事前検証や再起動が伴う物であり、迅速な適用は難しいという問題を解決するための手法である。なお、根本的な問題を解決できるわけではない、あくまで暫定対策であることに注意が必要である。

・提供元不明のソフトウェアを利用しない

・不要なサービスを停止または無効化する

停止するだけでなく、自動起動が有効になっていないことも確認しないと、サーバー再起動により起動されてしまうので確認する必要がある。

- アクセス権限管理を適切に行う

・アクセス権限を最小化する

不要なアカウントを作成せず、作成したアカウントに過剰な管理者権限や更新権限を与えない。

・管理者権限の運用体制を整える

内部不正防止のため、IT の面以外の対策も行う。例えば、運用担当者の制限をすることや利用記録を残すこと、クロスチェックをする等、運用手順の面での対策も有効である。

・定期的にアカウントの棚卸を行う

・同一のアカウントを複数人で運用しない

・アクセスログを収集し監視する

インシデント発生時には過去に遡って調査できるよう、保存期間やログファイルの運用方法も組織の方針に併せて検討する必要がある。

・パスワードを適切に運用する

「共通対策」内、別項を参照

- セキュリティ製品を導入する

・セキュリティソフト

セキュリティソフトとは様々なセキュリティ機能が統合されたソフトウェアである。アンチウイルスや迷惑メールのフィルタリング、Web アクセスのフィルタリングをはじめ、製品によって様々な機能を搭載している。アンチウイルスに関しては特に、最初に導入するだけでなく、定期的なスキャンやパターンファイルの更新を行うように設定し、結果を確認することが必要である。

・EDR (Endpoint Detection and Response)

サーバー内の処理や外部との通信等の不審な振る舞いを検知することで迅速な対応を可能にできる。

・NDR(Network Detection and Response)

ネットワークトラフィック（通信量）を監視、分析することで不審な通信を検知し、迅速な対応を可能にできる。

・DLP (Data Loss Prevention)

特定のデータのコピー等持ち出しを検知し、ブロックする。例えば、管理対象のデータがメールに添付されている場合にアラートを出したりブロ

ックしたりすることで誤送信等、作業ミスによる漏えいの防止等も可能である。

・IDS (Intrusion Detection System)

不正侵入検知システムと呼び、ネットワーク通信を監視し、不審な通信が見つかった際に担当者へ通知を行う。自動でブロックする機能はないが、通知を受けることで、担当者が内容を確認し対応を開始する契機となる。

・IPS (Intrusion Prevention System)

不正侵入防止システムと呼び、ネットワーク通信を監視し、不審な通信が見つかった場合は担当者への通知だけでなく自動でブロックも行う。IDS よりリスクの低減はできるが正規の通信をブロックしてしまうおそれもあり、組織の方針を踏まえた上での選定が必要である。

・WAF (Web Application Firewall)

ウェブサーバーの前面またはウェブサーバー内に設置することで通信を監視し、Web サイトを保護する。IDS、IPS がネットワークレベルでの監視を行うのに対して WAF はアプリケーションレベルでの監視であるため、組み合わせて適用することでより強固な防御が可能になる。

・UTM (Unified Threat Management)

統合脅威管理と呼び、IDS や IPS の機能やファイアウォール、アンチウイルス等、他の機能も備えた製品である。1 つに統合されていることで運用コストや手間を低減することができる。

● ネットワーク

・ネットワークを分離し、個別遮断できるようにする

・ファイアウォールを設置し、アクセス制御する

どこから、どのサーバーに、どのサービスにアクセスを許可するのか必要最小限にする。

・プロキシサーバーを導入する

利用者認証を受けない外部への不正通信をブロックする。

・不要なポートを閉じる

● その他

・セキュリティのサポートが充実している製品を使う

導入するソフトウェアもパッチや回避策の提供が迅速である物を使用する。

・統合運用管理ツールを導入する

統合運用管理ツールとは社内ネットワーク機器やサーバー等の IT 機器を一元管理するツールである。様々な管理項目があり、セキュリティ管理機能ではシステムへのアクセス権限の管理やファイアウォールの構築、暗号化等が可能である。他にも様々な機能があるため、セキュリティ対策だけでなく導入するメリットは大きいといえるツールである。

・重要データやファイルを暗号化する

・外部記憶媒体の接続を制限する

・セキュリティ診断を行う

セキュリティベンダーから提供されている診断サービスはサーバーやネットワーク全体を診断でき、適切な助言を受けられるため実施を検討するとよい。

・ペネトレーションテストを行う

・ログを取得し、監視や解析する

システムログ、アプリケーションログ、サーバーへのアクセスログ、認証ログ、データベース操作ログ、通信ログ等の各種ログを取得し、監視や解析をすることで不審な振る舞いの迅速な検知だけでなく被害に遭った際の原因特定が可能になる。

また、ログの取得は、取得レベルや保管期間については事前に検討が必要である。特に、運用を外注するのであればログの取得や監視、解析に関する仕様や運用の確認を行う。

IPA ではウェブサーバーや SSH、FTP サーバーのログを解析することで攻撃と思われる痕跡を検出するためのツール（iLogScanner[3]）を無料で提供しているので利用を検討するとよい。

**参考資料**

1. サイバーセキュリティ経営ガイドライン 付録B（経済産業省）
https://www.meti.go.jp/policy/netsecurity/downloadfiles/CSM_Guideline_app_B-2.pdf
2. 国民のためのサイバーセキュリティサイト（総務省）
https://www.soumu.go.jp/main_sosiki/cybersecurity/kokumin/index.html
3. ウェブサイトの攻撃兆候検出ツール iLogScanner (IPA)
https://www.ipa.go.jp/security/vuln/iLogScanner/index.html

## ■適切なバックアップ運用を行う

データの破損の原因は記憶装置の故障やランサムウェア等のサイバー攻撃による暗号化だけではなく、運用時の操作ミスによる消去や誤った更新と多岐に渡る。失ったデータの復旧は困難であり、復旧には人手と時間を要する。しかし、バックアップを取得しておくことでこの被害を縮小することが可能である。迅速にデータを復旧し業務継続できなければ、組織の信頼も失墜し、存続の問題に繋がりかねない大きなリスクとなる。そこで本項では適切なバックアップ運用について解説するので今後の運用の参考にしてほしい。

● バックアップを取得する

・対象を選定する

バックアップの対象は業務データだけではない。システムの稼働に必要な設定ファイルや、プログラムも含め、バックアップ対象を選定する。

・取得方法や取得日時、間隔を検討する

サーバーの稼働要件に併せてオフライン、オンラインバックアップのどちらか検討する。

対象のデータごとに適切な取得日時、間隔を検討する。例えば、業務データは週に1回フルバックアップ、その他の日に差分バックアップをする。プログラムファイルはシステム改修が無い限り変更はないためリリース時のみバックアップをする。設定ファイルは随時変更があるため週に1回取得する等のように検討する。

● バックアップを保管する

・3-2-1 ルール(3-2-1-1-0 ルール [1])

データはコピーして 3 つ持ち、2 種類のメディアでバックアップを保管し、バックアップの 1 つは違う場所で保存するというルールがある。ランサムウェアに対しては 3-2-1-1-0 ルールも提唱されているので参考にするとよい。

・保管場所を検討する

ランサムウェア攻撃に備えて、ネットワーク上隔離された場所へ保管する。外部記憶装置に保管し、バックアップ取得時以外は物理的に接続を切ることが望ましい。さらに、災害対策も含めるのであれば地理的に離れた異なるセンター内で保管するとさらによい。

・世代管理を行う

最新だけでなく、過去のバックアップも保管し、複数の時点にリカバリできるようにしておくことが望ましい。データの破損からそれを認知するまでに時間がかかると最新のバックアップもすでに破損しているおそれもあるためである。

また、バックアップにはいつ時点のどのデータが含まれているのか、ファイルの名称や保管している外部記憶装置を判別できるようにする。それらを扱う際の運用手順を定めることで誤った上書きや消去してしまうといった事故を防ぐ。

・保管期間を決める

バックアップの保管方法や世代管理と合わせて組織の方針を満たせる保管期間を決定する。

● バックアップからリカバリする

・リカバリ計画を立てる

バックアップは取得するだけで終わりではなく、それを利用していかに早く復旧するかが重要である。そのために想定される障害とその被害をあらかじめ考え、それぞれに対して復旧する時点やリカバリ手順を確立する。

・リカバリ訓練を行う

計画に基づいて正しく作業できるか定期的に訓練を行い、計画の見直しを行う。

● PC やスマートフォンを使う個人の対策

・大切なデータは別の媒体にも保存しておく

普段使用する端末とは別の端末や外付けハードディスク、SD カード等にデータを保存する。使わない時は保存した媒体と普段使用する端末は接続せずに保管する。

**参考資料**

1. Data Backup Options (アメリカ合衆国サイバーセキュリティ・社会基盤安全保障庁)
https://www.cisa.gov/uscert/sites/default/files/publications/data_backup_options.pdf


著作・制作　　独立行政法人情報処理推進機構（IPA）

執筆者　　内海　百葉　　亀山 友彦　　土屋　正

イラスト製作　　株式会社 創樹

**執筆協力者**　　**10 大脅威選考会**

**IPA 執筆協力者**　　**高柳　大輔**　　**桑名 利幸**　　**渡辺 貴仁**

# 情報セキュリティ対策の基本と共通対策

## 情報セキュリティ 10 大脅威 2023 版

---

2023 年 2 月 28 日　　初　版

[事務局・発行]　　独立行政法人情報処理推進機構

〒113-6591

東京都文京区本駒込二丁目 28 番 8 号

文京グリーンコートセンターオフィス

https://www.ipa.go.jp/