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 2024 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

2024 年 2 月

本資料は、以下の URL からダウンロードできます。

「情報セキュリティ 10 大脅威 2024」
https://www.ipa.go.jp/security/10threats/10threats2024.html

目次

「情報セキュリティ対策の基本」が重要

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、これらが利用する「攻撃の糸口」は似通っており、脆弱性を突く、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、被害に遭う可能性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 ※「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＋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。）

また、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上で参考としてほしい。なお、共通対策を実施すれば完全な対策になるというものではない。各脅威の解説も参照し、対策を実施することが重要である。

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、 メールや SMS のリンク、URL のクリックを 安易にしない	○	○
適切な報告／連絡／相談を行う	○	○
インシデント対応体制を整備し対応する		○
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		○
適切なバックアップ運用を行う	○	○

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/10threats/2015/2015.html

パスワードを適切に運用する

個人や組織に関わらず、オンラインショッピングや SNS を利用したり、AppleID や Google アカウントを利用したりする機会が増え、様々な場面でパスワードの設定が必要になる。推測可能なパスワードの設定や不適切な管理をすると、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 機器では出荷の際、共通したパスワードが初期設定さ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ことが有効である。内閣サイバーセキュリティセンター（NISC）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 ID とパスワードを同じ文字列にしない
② 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
③ 生年月日や名前を使わない
④ 連続した数字やアルファベットにしない
⑤ 単純な単語一語だけにしない

表 1.6　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 p@ssw0rd	単純な単語や 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

・パスワードを使い回さない

個人情報や金銭情報を登録しているサービスや、登録したメールアドレスを ID として利用するサービスでは、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、いずれかのサービスでパスワードの漏えいが起きたとき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作成時は参考にするとよい。[4]

・パスキーを利用する

パスキーと呼ばれる、生体情報等で認証を行う方式が提供されていれば利用するとよい。（詳細はコラムを参照すること）

● 適切な保管、運用を行う

・パスワードは他人に教えない

・PC やスマートフォンにパスワードを書いた付箋等のメモを貼らない

PC やスマートフォンを紛失した際に簡単に不正ログインされてしまう。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。

・複数人で使用する PC 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 PC 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ときの対応

・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。

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[1]に反することを行ったり、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規則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に影響が及ぶこと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人は気を付けるべきこと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 やスマートフォンを使う子へ[2]、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】

① SNS 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。

拡散する場合は一次情報を探し、発信者や発信内容が正しいのかファクトチェック等も活用して確認した上で拡散する。[3]

・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。情報を拡散する場合と同様に情報が正しいか確認した上で発信する。

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ばれている)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

・本物を騙った偽の Web サイトがある

・個人情報を盗もうとする Web 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ときには注意が必要である。

【組織】

① 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 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。[4, 5]

③ 教育受講者への意識付け

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、社内運用規則を理解すること

・事故を起こさないことは自身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、中途社員、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。これらを考慮した上で、毎回同じ教育コンテンツではなく、従業員の行動やポリシーを定期的に評価し、コンテンツを定期的に見直すことも必要である。

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

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、それに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。

● 被害に遭うタイミング

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、PC やスマートフォンがウイルス感染したりする可能性は低い。そのメールや SMS から誘導された Web サイトに情報を入力することで入力した情報が盗まれたり、添付ファイルを開くことでウイルス感染してしまったりする。

ウイルスに感染すると PC やスマートフォンに保存されている情報が盗まれたり、PC やスマートフォン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

メールや SMS、SNS で受信したメッセージ内のリンクを安易にクリックやタップをしない、QR コードを安易に読み取らないようにする。メール本文に記載されている URL をブラウザに安易に入力して開かないようにする。

これらの方法で開いた Web サイトは、正規の物を騙った偽物のおそれがある。

・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 Web サイトが開く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。

Microsoft Word や Excel を開いてしまった際に「マクロを有効にする」「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り、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。そのため、業務でマクロ機能を使用しない場合は、マクロを無効化しておくとよい。他にも、開いたファイルが安全ではないおそれがある場合に「編集を有効にする」というボタンが表示されることもある。これらのボタンを安易にクリックやタップはしないように注意が必要である。

● 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ください。」

「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は使用せず、以下のようにして正規の情報を確認するとよい。

① 事前にブックマーク（お気に入り）に登録しておく

よく利用している Web 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

② 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

③ Web サイトを検索して開き、確認する

対象のサービスをブラウザで検索して正規の Web サイトを開く。そして、例えば不在通知なら

ば追跡番号で調べるか問い合わせをする。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。

IPA では実際の画面を用いて紹介しているので、是非 IPA の Web サイトで手口を確認し、不審なメールや SMS に備えてほしい。[1]

適切な報告／連絡／相談を行う

【個人】

被害を受けたとき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。不安に感じたときや被害に遭ったときは慌てず、まずは落ち着いて、以下の相談先に連絡することが望ましい。

表 1.7【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 不審な Web サイトを見つけた 不審な Web 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 ②迷惑メール相談センター（日本データ通信協会） (https://www.dekyo.or.jp/soudan/index.html) ③サービス提供会社 ※不審なメールや SMS のリンクはクリックせず、不審な Web 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直して問い合わせる 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） ⑤フィッシング対策（警察庁） (https://www.npa.go.jp/bureau/cyber/countermeasures/phishing.html) 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 ②都道府県警察本部のサイバー犯罪相談窓口 (https://www.npa.go.jp/bureau/cyber/soudan.html)
クレジットカードを勝手に使われた インターネットバンキングで不正送金された ※③と④に連絡 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 ※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） ②勝手に使われたサービスや商品の提供会社 ③金融機関 ④都道府県警察本部のサイバー犯罪相談窓口 (https://www.npa.go.jp/bureau/cyber/soudan.html)
PC やスマートフォン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。 ①信頼できる知人 ②IPA（安心相談窓口） (https://www.ipa.go.jp/security/anshin/about.html)
自身のアカウントに勝手にログインされた	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インターネット上の誹謗中傷への対策（総務省） (https://www.soumu.go.jp/main_sosiki/joho_tsusin/d_syohi/hiboutyusyou.html) ②ネットの誹謗中傷（セーファーインターネット協会） (https://www.saferinternet.or.jp/bullying/) ③誹謗・中傷が掲載されている Web サイトや SNS の提供会社 ④都道府県警察本部のサイバー犯罪相談窓口 (https://www.npa.go.jp/bureau/cyber/soudan.html) ⑤弁護士、日本司法支援センター法テラス（https://www.houterasu.or.jp/）
上記のどれに当てはまるか分からない	①IPA（安心相談窓口） (https://www.ipa.go.jp/security/anshin/about.html) 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】

組織においては上司や責任者、経営者層に適切な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、外部からは隠蔽したとみなされ、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するとよい。

表 1.8【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。 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。 ①上司や責任者、セキュリティの管理者にエスカレーションする ※自身がインシデントを起こした、発見した場合 ②システム管理者にエスカレーションする ※自身が利用している PC やスマートフォン、システムに関するインシデントの場合 ③CSIRT にエスカレーションする ※組織内で CSIRT が構築されている場合
上司や責任者	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、組織内の関連部署へ横展開する。
経営者層や組織として	組織として、自組織や関係者の被害拡大防止、社会的責任を果たすために、外部へ報告、相談、公表する必要がある。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。 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） ※自組織だけでは調査や解決できない場合 ②顧客、取引先、委託先、委託元、関連組織に報告する ※場合によってはメディアへの公表を検討する ③金融機関、クレジットカード会社へ連絡する ※情報漏えい等によるさらなる被害拡大防止 ④監督省庁、IPA、JPCERT/CC に報告する ※発生したインシデントに併せて公的機関等に報告する J-CRAT 標的型サイバー攻撃特別相談窓口 (https://www.ipa.go.jp/security/todokede/tokubetsu.html) コンピュータウイルス・不正アクセスに関する届出 (https://www.ipa.go.jp/security/todokede/crack-virus/index.html) JPCERT/CC インシデント対応依頼 (https://www.jpcert.or.jp/form/) ⑤個人情報保護委員会に報告する ⑥警察に相談する ⑦弁護士に相談する

インシデント対応体制を整備し対応する

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。特に、サイバー攻撃を受けた際はより迅速な対応が必要である。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について解説するので、自組織における対応計画を作成する参考としてほしい。

【組織】

● 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

インシデント対応を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対応フローを確立し、連絡先を明確にした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の規則やポリシーの整備、予算の確保を経営者層が主体となって行う

● インシデント対応として CSIRT が行うべきこと

① 検知／連絡受付

セキュリティ機器での検知や組織内外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、速やかな対応を必要とする場合や情報共有をすべき場合は注意喚起や情報発信を適切に行う。

③ インシデントレスポンス

対応すべきと判断したインシデントを分析し、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実施し、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、監督省庁への報告を行う。

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]

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

組織に対する脅威はサーバーやクライアント、ネットワークに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、今後も攻撃者から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、組織のサーバーは例えば、「更新プログラム適用」ひとつとっ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。

【組織】[1,2]

● 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

自組織で使用している製品のサポート期限を把握しておき、サポート切れになる前に移行計画を立てて運用を検討する。

・提供元不明のソフトウェアを利用しない

・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。

特に、利用しているソフトウェアの管理においては SBOM の導入を検討する。[3]

また、誰が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

・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。そのため、迅速に更新プログラムを適用できない場合に、ネットワークレベルで攻撃の通信を遮断することで一時的に問題を解決する手法が仮想パッチである。根本的な問題を解決できるわけではなく、あくまで暫定対策であることに注意が必要である。

・不要なサービスを停止または無効化する

サーバー再起動により、停止したサービスが自動起動されないよう、自動起動が無効の設定になっていることを確認する。

● 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 を伴わない対策も行う。例えば、運用担当者を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こと等、運用方法で対策することも有効である。

・定期的にアカウントの棚卸を行う

従業員や職員の離任時に対象者のアカウントを削除し、その上で定期的に棚卸を行うことで、権限付与の妥当性や、不要なアカウントが存在していないか等を確認する。

・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（詳細は「共通対策_パスワードを適切に運用する」を参照すること。）

・多要素認証の設定を有効にする

利用している機器が多要素認証に対応している場合は設定を有効にしておくことで不正アクセスを防止する。

● 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。特にアンチウイルスに関しては、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)

サーバーおよびクライアント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する。

・NDR (Network Detection and Response)

ネットワーク上の通信を監視、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。

・CSPM (Cloud Security Posture Management)

クラウドの設定ミスによる情報漏えいを防ぐ。あらかじめ自社のポリシーを元にチェックのルールを設定しておき、そのルールに抵触する設定がなされた場合にアラートを出すことで設定ミスに気が付けるようにする。

・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。

・DNS フィルタリング

新しく登録された未検証のドメインや不審なドメイン、悪性な類似ドメインへのアクセスを名前解決の段階で防止する。

・WAF (Web Application Firewall)

Web サーバーの前面または Web 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期待できる。

● ネットワーク管理を適切に行う

・ネットワークの分割と個別遮断を行う

ネットワークを事業所や部署、機器の用途などの単位等で論理的、もしくは物理的に分割する。インシデントが発生した際は分割されたネットワークを隔離することでウイルス感染時の被害を局所化する。

・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させるかを検討し、必要最小限のアクセス制御を行う。

・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。

・ASM（Attack Surface Management）を行う

ASM とは組織の外部（インターネット）からアクセス可能な IT 資産を発見し、それらに存在する脆弱性などのリスクを継続的に検出・評価する一連のプロセスのことである。組織管理者の未把握の機器や意図しない設定ミスを攻撃者視点から発見でき、脆弱性管理活動において、リスク低減の効果が期待できる。[4]

・不要なポートへの通信や不要なプロトコルの通信は遮断する

● 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設定、暗号化方式の選択等が可能である。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ことにより、大きなメリットを期待できるツールである。

・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

・脆弱性診断を行う

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

実際の攻撃シミュレーションを通じてセキュリティ体制の実効性を評価する。

・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、ログレベルや保管期間について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 Web 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[5]）を無料で提供しているので利用を検討するとよい。

・サイバーセキュリティお助け隊サービス

「見守り」「駆付け」「保険」など中小企業のセキュリティ対策に不可欠なワンパッケージのサービスを要件としてまとめ、これを満たすことが所定の審査機関により確認された民間サービスを IPA で公表している。これを活用してワンパッケージで安価にセキュリティ対策を行う。[6]

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軽減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 [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。[2]

・保管場所を検討する

ランサムウェア攻撃に備えて、ネットワーク上から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場所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、複数の時点に復旧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があるためである。

また、バックアップにはいつの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て上書きしてしまったり、消去してしまったりする事故を防ぐ。

・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ストアする

・復旧計画を立てる

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ストア手順を確立する。

・正しく復旧できることを確認する

計画に基づいて正しく復旧できるか定期的に確認し、必要に応じて手順の見直しを行う。

● 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 PC やスマートフォン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 PC やスマートフォンとは接続せずに保管する。

参考資料

【共通対策】

・「パスワードを適切に運用する」

1. 不正ログイン対策特集ページ（IPA）
   https://www.ipa.go.jp/security/anshin/measures/account_security.html
2. チョコっとプラスパスワード（IPA）
   https://www.ipa.go.jp/security/chocotto/index.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/attention/2016/mgdayori20160803.html

・「情報リテラシー、モラルを向上させる」

1. 第5章　情報モラル教育（文部科学省）
   https://www.mext.go.jp/b_menu/shingi/chousa/shotou/056/shiryo/attach/1249674.htm
2. ファクトチェックとは（認定NPO法人　ファクトチェック・イニシアティブ）
   https://fij.info/introduction
3. 情報セキュリティ関連サイト（IPA）
   https://www.ipa.go.jp/security/guide/keihatsu.html
4. サイバーセキュリティのひみつ（IPA）
   https://www.ipa.go.jp/security/security-himitsu/index.html
5. 対策のしおり（IPA）
   https://www.ipa.go.jp/security/guide/shiori.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. 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/attention/2021/mgdayori20210831.html

・「インシデント対応体制を整備し対応する」

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. サイバーセキュリティ経営ガイドライン　付録B－2（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. 「ソフトウェア管理に向けたSBOM（Software Bill of Materials）の導入に関する手引」を策定しました（経済産業省）
   https://www.meti.go.jp/press/2023/07/20230728004/20230728004.html
4. 「ASM（Attack Surface Management）導入ガイダンス～外部から把握出来る情報を用いて自組織のIT資産を発見し管理する～」を取りまとめました（経済産業省）
   https://www.meti.go.jp/press/2023/05/20230529001/20230529001.html
5. 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
6. サイバーセキュリティお助け隊サービス（IPA）
   https://www.ipa.go.jp/security/otasuketai-pr/index.html

・「適切なバックアップ運用を行う」

1. Data Backup Options（サイバーセキュリティ・インフラストラクチャセキュリティ庁）
   https://www.cisa.gov/sites/default/files/publications/data_backup_options.pdf
2. What is the 3-2-1 backup rule?（Veeam Software）
   https://www.veeam.com/blog/321-backup-rule.html

著作・制作　　独立行政法人情報処理推進機構（IPA）

執筆者　　篠塚　耕一　　内海　百葉　　亀山　友彦　　土屋　正

イラスト製作　　株式会社 創樹

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 2024 版

2024 年 2 月 29 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/