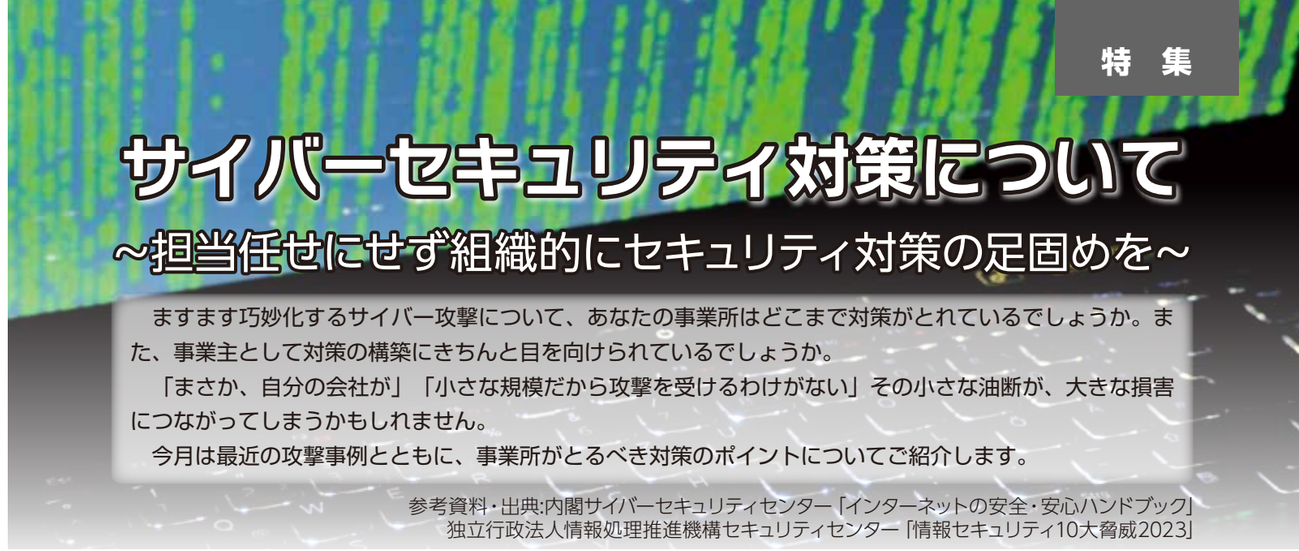

サイバーセキュリティ対策について

～担当任せにせず組織的にセキュリティ対策の足固めを～

ますます巧妙化するサイバー攻撃について、あなたの事業所はどこまで対策がとれているでしょうか。また、事業主として対策の構築にきちんと目を向けられているでしょうか。

「まさか、自分の会社が」「小さな規模だから攻撃を受けるわけがない」その小さな油断が、大きな損害につながってしまうかもしれません。

今月は最近の攻撃事例とともに、事業所がとるべき対策のポイントについてご紹介します。

参考資料・出典:内閣サイバーセキュリティセンター「インターネットの安全・安心ハンドブック」
独立行政法人情報処理推進機構セキュリティセンター「情報セキュリティ10大脅威2023」

情報セキュリティの10大脅威（組織編）

①ランサムウェアによる被害 ～猛威を振るうランサムウェア、複数の脅迫で被害者を逃がさない～

ランサムウェアと呼ばれるウイルスにサーバー等が感染すると、データの暗号化等が行われたり、重要な情報を窃取されたりし、その復旧と引き換え、もしくは情報を公開すると脅したりして金銭を要求し、企業が支払わざるを得ない状況を作り出そうとします。

②サプライチェーンの弱点を悪用した攻撃 ～自組織だけでなく、委託先や利用しているサービスも適切管理を～

セキュリティ対策が強固な企業・ソフトウェアは攻撃せず、対策が脆弱なプロセスを標的にし、踏み台として顧客・上流プロセスの関連企業等、本命の標的を攻撃します。

③標的型攻撃による機密情報の窃取 ～メールが来たらまずは疑え！？意識は常に高く～

機密情報を窃取することや業務妨害を目的に、特定の組織（官公庁、民間団体、企業等）を狙う攻撃。

④内部不正による情報漏洩 ～不正に情報を取得しない、取得させない、使用しない～

悪意を持った内部関係者が、金銭目的や私怨を理由に、組織が保管する技術情報や顧客情報等の重要情報を不正に持ち出し、不特定多数が閲覧できる場所に公開したり、競合他社へ有利に転職するために情報提供します。

⑤テレワーク等のニューノーマルな働き方を狙った攻撃 ～未だ脆弱なテレワーク環境が狙われる～

テレワーク用に導入している製品の脆弱性や設定ミス等を悪用し社内システムに不正アクセスしたり、ＰＣ内の業務情報等を窃取したりします。また、ウェブ会議サービスの脆弱な設定を悪用し、ウェブ会議をのぞき見します。また、適切なセキュリティ対策が行われていない自宅やオフィスで端末を利用し情報を窃取されます。

⑥修正プログラムの公開前を狙う攻撃 ～事前に防ぐことは困難。悪用の情報が公開されたら即時対応を～

ＯＳやソフトウェアに脆弱性の存在が判明し、その修正プログラムや回避策がベンダーから提供される前に、その脆弱性を悪用してサイバー攻撃が行われることがあります。

⑦ビジネスメール詐欺による金銭被害 ～そのメール、相手がだれか分かりますか？～

悪意のある第三者が取引先や自社の経営者等になりすまし、偽のメールを送ったり組織間のメールのやり取りを乗っ取ったりしたうえで、最終的に偽の銀行口座に送金させるサーバー攻撃です。

⑧脆弱性対策情報の公開に伴う悪用増加 ～「後で対応しよう」、その数日が命取り～

ソフトウェアやハードウェアの脆弱性対策情報の公開を悪用し、脆弱性対策を講じていないシステムを狙って攻撃を行います。近年では脆弱性情報の公開後に攻撃コードが流通し、攻撃が本格化するまでの時間が短くなっており、より迅速な対応が求められます。

⑨不注意による情報漏洩等の被害 ～一つのうっかりが大事件につながることも～

メールの誤送信や記憶媒体の紛失等の不注意により個人情報が漏洩し、その情報が第三者に売買されさらなる悪用につながり、組織は社会的信頼の失墜や経済的な損失につながる恐れがあります。

⑩犯罪のビジネス化（アンダーグラウンドサービス） ～攻撃者もショッピング。商品はあなたの情報～

犯罪に使用するためのサービスやツール、ＩＤやパスワードの情報等がアンダーグラウンド市場で取り引きされ、これらを悪用した攻撃が行われています。専門知識が無い者でもサービスやツールを利用することで容易に攻撃が行えるため、サービスやツールが公開されると被害が広がる恐れがあります。

攻撃者が利用する「攻撃の糸口」は似通っており、５つに分類することができます。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」としており、この対策を意識して継続的に行うことで、被害に遭うリスクを低減できると考えられています。

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	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

【複数の脅威に有効な対策】

●パスワードを適切に運用する

・初期設定のままにしない
・『絶対に』使いまわさない
・適切な保管、運用を行う（メモを端末に貼らない、ブラウザにパスワードを記憶させない等）
・英大文字小文字＋数字＋記号で10桁以上

●情報リテラシー、モラルを向上させる（従業員教育）

・掲載されている情報が正しいとは限らない
・安易に情報を拡散せず慎重に
・「本物に似せたウェブサイト」「個人情報を盗もうとするウェブサイトがある」ことを知る
・情報リテラシーや情報モラルの向上を図る
・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

なお、教育する際は▽他人事と考えない▽就業規則、社内運用規則を理解する▽事故を起こさないことは自分を守ることでもあること▽緊急時の報告先、報告方法を把握すること、等を意識付けすることが必要です。また、人の入れ替わりなどを考慮し、定期的に、適切な時期に教育機会を設けるようにしましょう。

●メールの添付ファイルの開封、メールやＳＭＳのリンク、ＵＲＬのクリックを安易にしない

・よく利用しているウェブサイトはブックマークし、そこからアクセスする
・正規のアプリをインストールしておき、そのアプリを使う
・不在通知なら追跡番号で調べる

●インシデント対応体制を整備し対応する

・専門知識を持つ責任者を配置する、もしくはインシデント対応の統制をする責任者を決めておく
・有事の際の連絡先や対応フォロー等、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（訓練）する
・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
・継続的に行える体制と社内の規則やポリシーの整備、予算の確保を行う

●適切な報告・連絡・相談を行う

報告・連絡・相談先の事例

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。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(※)しないと隠ぺいを疑われるので、躊躇せずにエスカレーションすることが重要。 〈相手〉上司・セキュリティ管理者・システム管理者 等
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。日ごろから関係者を把握し対応手順を理解しておくことが重要。 〈相手〉組織内の関連部署へ横展開、組織外への情報発信を検討・判断
経営者・組織として	被害拡大防止や原因と対応の報告を1次・2次と段階を分けて適切に行うことが重要。 〈相手〉セキュリティ専門会社、顧客・取引先・委託先等への報告、金融機関・クレジット会社への連絡、警察へ被害届の提出、監督省庁に報告、弁護士に相談

（※）何らかのアクシデントが起きた際、上司に報告・相談し、判断を仰ぐこと。