国土交通省所管インフラ分野向け

情報セキュリティ対策　チェックリスト

令和７年５月　第１版

国土交通省総合政策局

情報政策課サイバーセキュリティ対策室

目　　次

1 はじめに

本チェックリストは、国土交通省が所管する企業や自治体等を主な対象とし、企業等の担当者が自社等の業種や規模に応じた適切なセキュリティ対策を実施できるよう作成しました。企業等の情報を守り、サイバー攻撃や情報漏えいのリスクを減らすことを目的としています。

本チェックリストにつきましては、平成３０年３月に初版を公表し、第２版では企業へサイバーセキュリティ対策の状況についてのアンケート調査を実施し、その結果を基に見直しを行いました。第２版までは業種ごとに異なるチェックリストを提供していましたが、本チェックリスト（第３版）では、より包括的で統一されたチェックリストを提供するために、業種別の構成を統合し、１つのチェックリストにまとめました。これにより、企業等の業種や規模を問わない共通の基準でもセキュリティ対策の状況を評価し、改善に役立てることが可能となっております。

本チェックリストを活用することで、情報セキュリティ対策の現状を評価し、継続的な改善を図ることで、各企業等のセキュリティ対策レベルが向上することを期待しています。

2 チェックリストの目的

本チェックリストは、主に以下の目的で活用できます。

- セキュリティ対策の現状を手軽に確認が出来る
- 必要と考えられる対策のおさらいにより対策を見落とさないようにする
- セキュリティルールや対策計画を作る際の参考にする
- 定期的なセキュリティ対策の見直しに役立てる

3 チェックリストの使い方

- 本チェックリストの作成にあたっては、業種別にセキュリティ対策やリスク認識などの実態を調査し、業界に特有のリスクや対策の傾向を分析しています。
- 本チェックリストは、以下の 2 部構成になっており、①から順にチェックを行うことで、セキュリティレベルごとの実施状況を把握できます。
- 各項目にはリスクと対策の例を記載しており、セキュリティ対策の特徴を参考にチェックできるようにしています。
- 実施できていない項目については、対策に参考となる情報の例などを参照し、自社等に適したセキュリティ対策を進めてください。

■チェックリストの構成

①実施すべき基本的なセキュリティ対策を整えたい企業等向け

- 最低限実施すべきと考えられる基本的な対策を含みます。
- セキュリティ対策を基本から見直したい企業等向けです。

②セキュリティ対策をレベルアップさせたい企業等向け

- 基本的な対策が整っている企業等のために、より強固なセキュリティ対策を実施するための項目です。

■チェックリスト活用上の注意点

- セキュリティレベル別のチェック項目の分類は参考です。
- すべての企業等に当てはまるわけではなく、企業等ごとのシステム環境や業務内容によって適宜必要な項目を参照してください。
- チェックリストの対策をすべて行ったとしても対策は完全とは限りません。
- 各企業等の実情に応じた適切なセキュリティ対策を講じ、継続的な改善を図ってください。

4 チェックリスト

①実施すべき基本的なセキュリティ対策を整えたい企業等向け（目的：最低限実施すべきと考えられる基本的な対策を確保する）

No	チェック項目	想定されるリスクの例	対策の例	対策に参考となる情報の例
1	**会社等のセキュリティルールを決め、従業員に説明していますか？**	ルールが不明確だと、情報漏洩や不適切な行動が発生する可能性があります。	セキュリティガイドを作成し、入社時に配布するなど	・中小企業の情報セキュリティ対策ガイドライン第 3.1 版 P26 (3)情報セキュリティ規程の作成 ・国民のためのサイバーセキュリティサイト システムを“管理”する人向けの対策 P3 情報セキュリティ関連文書の整備
2	**従業員向けに、定期的なセキュリティ教育を行っていますか？**	知識が不足するとミスが増え、ウイルス感染や情報漏洩などのトラブルが発生しやすくなります。	年 1 回の研修や、注意喚起のメール配信を実施するなど	・インターネットの安全・安心ハンドブック Ver 5.10 P160 7.10 従業員・職員等の利用者に対する情報教育等を怠らない ・国民のためのサイバーセキュリティサイト システムを“管理”する人向けの対策 P18 セキュリティ啓発活動・教育の実施 ・組織における内部不正防止ガイドライン 第 5 版 P72～74 (20)教育による内部不正対策の周知徹
3	**過去のセキュリティ事故や事例を社内で共有していますか？**	共有しないと、同じようなトラブルが繰り返し発生する可能性があります。	事例をメールや朝礼等で共有し、対策を確認するなど	・中小企業の情報セキュリティ対策ガイドライン第 3.1 版 P33 (1)情報収集と共有
4	**業務上知り得た情報の扱いについて、従業員に教育し、守られているか確認していますか？**	機密情報が外部に流出すると、企業等の競争力が低下したり、法的トラブルが発生したりする可能性があります。	守秘義務について説明し、誓約書を取り交わすなど	・中小企業の情報セキュリティ対策ガイドライン第 3.1 版 P33 (1)情報収集と共有 ・組織における内部不正防止ガイドライン 第 5 版 P78 (22)派遣労働者による守秘義務の遵守
5	**SNS への不適切な投稿や情報漏洩を防ぐためのルールを決めていますか？**	従業員の投稿が原因で企業等の信用が低下したり、個人情報が流出するリスクがあります。	業務に関する投稿を禁止するルールを明確にするなど	・インターネットの安全・安心ハンドブック Ver 5.10 P23 7 SNS やネットのコミュニケーションや発信時に注意したいことは？ ・組織における内部不正防止ガイドライン 第 5 版 P54～57 (13)ネットワーク利用のための安全管理
6	**強力なパスワードを設定し、使い回しを避けていますか？**	短くて単純なパスワードを使用すると、不正アクセスやアカウント乗っ取りの危険があります。	英数字・記号を含む長いパスワードを設定し、定期的に変更するなど	・インターネットの安全・安心ハンドブック Ver 5.10 P31～33 3 ②パスワードは長く複雑にして、他と使い回さないようにしよう ・組織における内部不正防止ガイドライン 第 5 版 P44 (7)情報システムにおける利用者の識別と認証

No	チェック項目	想定されるリスクの例	対策の例	対策に参考となる情報の例
7	**退職者や異動者のアカウントをすぐに削除・権限変更していますか？**	放置されたアカウントが悪用され、不正アクセスや情報漏洩のリスクが高まります。	退職日や異動日にアカウントを無効化・権限変更し、必要なデータを管理者や後任者が引き継ぐなど	・インターネットの安全・安心ハンドブック Ver 5.10 P151 6.3 問題が起きると事業継続に影響を及ぼす ・国民のためのサイバーセキュリティサイト システムを“管理”する人向けの対策 P22～23 アカウント管理 ・組織における内部不正防止ガイドライン 第 5 版 P81～82 (24) 雇用終了及び契約終了による情報資産等の返却
8	**席を離れるときに画面ロックをするよう徹底していますか？**	パソコンを勝手に操作されると、情報が盗まれたり改ざんされたりするリスクがあります。	一定時間操作しないと自動でロックがかかる設定をするなど	・インターネットの安全・安心ハンドブック Ver 5.10 P42～43 7 ⑥スマホやパソコンの画面ロックを利用しよう
9	**個人のスマホやパソコンを業務で使う場合、セキュリティ対策を行っていますか？**	会社等の管理が及ばず、情報漏洩やウイルス感染のリスクが高まります。	端末にパスワードや生体認証を設定し、業務データはクラウドで管理、OS やアプリを最新の状態に保つなど	・中小企業の情報セキュリティ対策ガイドライン第 3.1 版 P44 個人所有のパソコンやスマートフォンをテレワーク端末として利用する場合 ・インターネットの安全・安心ハンドブック Ver 5.10 P142 3.1 テレワークと BYOD-Bring Your Own Device ・組織における内部不正防止ガイドライン 第 5 版 P50～51 (11)個人の情報機器及び記録媒体の業務利用及び持込の制限
10	**ウイルス対策ソフトを導入し、定期的に更新していますか？**	最新の対策をしていないと、ウイルスやランサムウェアに感染し、データの漏洩や消失の危険があります。	ウイルス定義を最新の状態に保つ設定にするなど ※ 外部ネットワークから物理的に分離されている場合など、本対策を必要としない環境もあります	・インターネットの安全・安心ハンドブック Ver 5.10 P135～138 1 社内・社外のセキュリティを向上しよう ・国民のためのサイバーセキュリティサイト システムを“管理”する人向けの対策 P8～10 マルウェア（ウイルス等）対策管理
11	**OS やソフトウェアの更新（アップデート）を定期的に実施していますか？**	古いソフトを使い続けると、脆弱性を悪用され、不正アクセスや攻撃を受ける可能性があります。	OS やソフトウェアの更新情報を都度入手出来る環境にして適宜必要な更新を行う、不要なソフトは削除するなど ※ 外部ネットワークから物理的に分離されている場合など、本対策を必要としない環境もあります	・インターネットの安全・安心ハンドブック Ver 5.10 P29 2.1 パソコン本体とセキュリティの状態を最新に保とう ・国民のためのサイバーセキュリティサイト システムを“管理”する人向けの対策 P6～7 ソフトウェアの最新化・脆弱性管理
12	**Wi-Fi のセキュリティ設定を適切に管理していますか？**	セキュリティが弱いと、不正アクセスや通信の盗聴が発生し、情報が漏洩する恐れがあります。	初期パスワードを変更し、WPA2（Wi-Fi Protected Access 2）以上の暗号化を設定するなど	・インターネットの安全・安心ハンドブック Ver 5.10 P110～117 2 安全な無線 LAN の利用を支える暗号化について学ぼう ・組織における内部不正防止ガイドライン 第 5 版 P61～64 (16)組織外部での業務における重要情報の保護

No	チェック項目	想定されるリスクの例	対策の例	対策に参考となる情報の例
13	**USB メモリなどの外部デバイスの使用を制限していますか？**	許可なく USB メモリを使用すると、ウイルス感染や情報漏洩が発生する可能性があります。	業務用 USB メモリを限定し、管理方法を決めるなど	・中小企業の情報セキュリティ対策ガイドライン第 3.1 版 P62 手順 3 情報セキュリティ対策の決定 ・国民のためのサイバーセキュリティサイト システムを“管理”する人向けの対策 P10 USB メモリを介したマルウェア感染への対策 ・組織における内部不正防止ガイドライン 第 5 版 P47～48 (9)情報機器及び記録媒体の資産管理及び物理的な保護 P49 (10)情報機器及び記録媒体の持出管理 P50～51 (11)個人の情報機器及び記録媒体の業務利用及び持込の制限
14	**クラウドサービスのアクセス権限を適切に管理していますか？**	設定ミスや不正アクセスにより、クラウド上の機密情報が漏洩するリスクがあります。	不要なアカウントの削除や、アクセス制限を設定するなど	・中小企業の情報セキュリティ対策ガイドライン第 3.1 版 P38～41 (3)クラウドサービスの情報セキュリティ ・インターネットの安全・安心ハンドブック Ver 5.10 P144～145 4 ファイルの権限設定や情報の公開範囲を見直そう ・組織における内部不正防止ガイドライン 第 5 版 P61～64 (16)組織外部での業務における重要情報の保護
15	**フィッシングメールや不審なリンクに注意するよう、従業員に教育していますか？**	フィッシング攻撃やマルウェア感染が発生するリスクがあります。	怪しいメールを見つけたら報告するルールを作るなど	・インターネットの安全・安心ハンドブック Ver 5.10 P41 6 ⑤メールの添付ファイルや本文中のリンクに注意しよう P123～128 4 安全なデータファイルの利用を支える暗号化について学ぼう ・国民のためのサイバーセキュリティサイト システムを“管理”する人向けの対策 P11～14 電子メールにおけるセキュリティ対策
16	**メールの誤送信を防ぐため、送信前に宛先を確認していますか？**	誤送信によって機密情報が外部に流出し、信用を失うリスクがあります。	送信前に宛先を複数回確認するルールを設けるなど	・組織における内部不正防止ガイドライン 第 5 版 P54～57 (13)ネットワーク利用のための安全管理
17	**重要なデータのバックアップを定期的に取っていますか？**	バックアップがないと、ランサムウェア攻撃やシステム障害でデータを失う危険があります。	外付け HDD やクラウドストレージに定期的に保存するなど	・インターネットの安全・安心ハンドブック Ver 5.10 P44～45 8 ⑦大切な情報は失う前にバックアップ(複製)しよう ・国民のためのサイバーセキュリティサイト システムを“管理”する人向けの対策 P28～30 データ復旧・バックアップの管理

No	チェック項目	想定されるリスクの例	対策の例	対策に参考となる情報の例
18	**機密情報を含む書類やデータを適切に廃棄していますか？**	不適切な廃棄により、情報が第三者に流出する可能性があります。	シュレッダーを使用し、電子データは完全削除するなど	・国民のためのサイバーセキュリティサイト　システムを“管理”する人向けの対策 P4～5 安全なデータ・端末の廃棄 ・組織における内部不正防止ガイドライン 第５版 P47～48 （９）情報機器及び記録媒体の資産管理及び物理的な保護
19	**機密情報の取り扱いルールを決め、従業員に周知していますか？**	ルールがないと、情報が適切に管理されず、漏洩や不正利用のリスクが高まります。	機密情報の管理基準を文書化し、アクセス制限を設けるなど	・組織における内部不正防止ガイドライン 第５版 P114 対策のヒントとなる Q&A17
20	**個人情報の管理体制を整備し、適切に運用していますか？**	個人情報が不適切に扱われると、法的責任や罰則、損害賠償請求のリスクがあります。	個人情報の取り扱いルールを明確にし、必要な場合は暗号化するなど	・中小企業の情報セキュリティ対策ガイドライン第 3.1 版 P24～29 ４本格的に取り組む ・サイバーセキュリティ経営ガイドライン 経済産業省 P21～22 指示５ サイバーセキュリティリスクに効果的に対応する仕組みの構築 ・インターネットの安全・安心ハンドブック Ver 5.10 P161 ８個人情報は法律に則り適切に取り扱おう
21	**重要情報を持ち出す際、盗難や紛失の対策を実施していますか？**	紛失や盗難により、機密情報が外部に漏れるリスクがあります。	機密データを暗号化し、持ち出し記録を管理するなど	・サイバーセキュリティ経営ガイドライン 経済産業省 P50 (23)リスク対応（回避、低減、移転、保有） ・インターネットの安全・安心ハンドブック Ver 5.10 P90 2.2 暗号化機能などでセキュリティレベルを高める
22	**セキュリティインシデントが発生した場合の報告・対応ルールを明確にしていますか？**	迅速な対応ができないと、被害が拡大し、企業等の信用が低下するリスクがあります。	インシデント対応手順を決め、従業員に周知するなど	・中小企業の情報セキュリティ対策ガイドライン第 3.1 版 P46～47 (5)セキュリティインシデント対応 ・サイバーセキュリティ経営ガイドライン 経済産業省 P25～28 ３.３.インシデント発生に備えた体制構築 ・国民のためのサイバーセキュリティサイト　システムを“管理”する人向けの対策 P31～32 インシデントレスポンス体制整備
23	**重要エリアへの入退室管理を適切に行っていますか？**	不正侵入により、情報が盗まれたり、物理的な破壊行為が発生する可能性があります。	入退室記録を残し、許可された人のみが入れるようにするなど	・サイバーセキュリティ経営ガイドライン 経済産業省 P50 (23)リスク対応（回避、低減、移転、保有） ・組織における内部不正防止ガイドライン 第５版 P45～46 （８）物理的な保護と入退管理 P111 対策のヒントとなる Q&A9
24	**パソコン画面の覗き見を防ぐための対策を講じていますか？**	他人に画面を見られることで、機密情報が漏洩する恐れがあります。	プライバシーフィルターを使用し、機密情報が見えないようにするなど	・インターネットの安全・安心ハンドブック Ver 5.10 P46 ９⑧外出先では紛失・盗難・覗き見に注意しよう ・組織における内部不正防止ガイドライン 第５版 P61～64 (16)組織外部での業務における重要情報の保護
25	**重要な情報をやり取りする取引先との契約書に、秘密保持条項を明記していますか？**	契約の不備があると、情報漏洩が発生し、法的トラブルにつながる可能性があります。	契約書に秘密保持義務を明記し、定期的に見直すなど	・組織における内部不正防止ガイドライン 第５版 P78 (22)派遣労働者による守秘義務の遵守

No	チェック項目	想定されるリスクの例	対策の例	対策に参考となる情報の例
26	**委託先や協力会社等のセキュリティ管理状況を定期的に確認していますか？**	委託先のセキュリティが不十分だと、情報漏洩やサプライチェーン攻撃のリスクが高まります。	セキュリティに関する契約を結び、定期的に確認するなど	・中小企業の情報セキュリティ対策ガイドライン第 3.1 版 P28 (4)委託時の対策 ・サイバーセキュリティ経営ガイドライン 経済産業省 P29～30 3.4.サプライチェーンセキュリティ対策の推進 ・インターネットの安全・安心ハンドブック Ver 5.10 P162 9 取引先の監督を徹底しよう
27	**Web サイトのセキュリティ対策を実施し、顧客の個人情報を適切に保護していますか？**	セキュリティ対策が不十分だと、個人情報やクレジットカード情報が盗まれ、不正利用されるリスクがあります。	TLS（Transport Layer Security。インターネット通信を暗号化してデータの盗聴や改ざんを防ぐ技術）を導入して通信を暗号化し、セキュリティに注意してサイトを作成するなど	・中小企業の情報セキュリティ対策ガイドライン第 3.1 版 P34～37 (2)ウェブサイトの情報セキュリティ ・国民のためのサイバーセキュリティサイト システムを“管理”する人向けの対策 P14～16 ウェブサイトにおけるセキュリティ対策 ・組織における内部不正防止ガイドライン 第 5 版 P37～39 4-2-1.秘密指定
28	**システムの動作やユーザーの操作を記録するログを適切に取得・管理していますか？**	ログを記録しないと、不正アクセスや障害の原因を特定できず、対策が遅れるリスクがあります。改ざんされると、不正の証拠が残らず被害が拡大する恐れがあります。	重要なシステムでは、アクセスログを自動記録し、一定期間保存する。改ざん防止のため、クラウドや専用サーバーに保存するなど。	・中小企業の情報セキュリティ対策ガイドライン第 3.1 版 P52～53 ログ管理 ・国民のためのサイバーセキュリティサイト システムを“管理”する人向けの対策 P25～27 監査ログの管理 ・組織における内部不正防止ガイドライン 第 5 版 P52～53 (12)内部不正モニタリングシステムの適用

② セキュリティ対策をレベルアップさせたい企業等向け（目的：より高度なセキュリティ対策を実施し、リスクを低減する）

No	チェック項目	想定されるリスクの例	対策の例	対策に参考となる情報の例
1	**セキュリティのルールを定期的に見直していますか？**	ルールを更新しないと、新たなリスクに対応できず、古い対策のままになってしまいます。	年に 1 回以上、会社の状況や新しい脅威に合わせてルールを更新するなど	・中小企業の情報セキュリティ対策ガイドライン第 3.1 版 P26～27 (3)情報セキュリティ規程の作成 ・国民のためのサイバーセキュリティサイト　システムを“管理”する人向けの対策 P3 情報セキュリティ関連文書の整備
2	**従業員ごとに個別の ID を使い、共用アカウントをなくしていますか？**	共用アカウントを使うと、誰が何をしたか分からず、不正利用を防ぎにくくなります。	すべての従業員に専用の ID を割り当て、ID の共有を禁止するなど	・中小企業の情報セキュリティ対策ガイドライン第 3.1 版 P52 ③アクセス管理 ・国民のためのサイバーセキュリティサイト　システムを“管理”する人向けの対策 P22～23 アカウント管理 ・組織における内部不正防止ガイドライン 第 5 版 P44 (７)情報システムにおける利用者の識別と認証
3	**重要なシステムには二要素認証（パスワード＋ワンタイムコードなど）を導入していますか？**	パスワードだけでは不正アクセスを防げず、情報が盗まれるリスクがあります。	クラウドサービスや社内システムのログイン時に二要素認証を設定するなど	・インターネットの安全・安心ハンドブック Ver 5.10 P102～103 1.6 二段階認証と二要素認証と多要素 認証の安全性
4	**従業員のアクセス権限を必要最小限に設定し、定期的に見直していますか？**	不要な権限を持つと、情報漏洩や誤操作のリスクが高まります。	業務に必要な権限だけを付与し、定期的に不要な権限を削除するなど	・国民のためのサイバーセキュリティサイト　システムを“管理”する人向けの対策 P24 アクセス制御・管理 ・組織における内部不正防止ガイドライン 第 5 版 P61～64 (16)組織外部での業務における重要情報の保護
5	**不正アクセスを検知する仕組みを導入していますか？**	不正アクセスを見逃すと、情報を盗まれたり、社内ネットワークに侵入されたりする危険があります。	セキュリティソフトや監視ツールで、不審なアクセスを検知できるようにするなど	・中小企業の情報セキュリティ対策ガイドライン第 3.1 版 P50～53 (7)技術的対策例と活用 ・インターネットの安全・安心ハンドブック Ver 5.10 P153～154 7.2 不正アクセスの傾向 P158 7.8 ウェブサイトの改ざんや SNS の乗っ取り
6	**特別な権限を持つ ID（特権 ID）の管理を徹底していますか？**	特権 ID が不正に使われると、システムを乗っ取られるリスクがあります。	特権 ID の利用を管理者などに制限し、使用履歴を記録・確認するなど	・中小企業の情報セキュリティ対策ガイドライン第 3.1 版 P52 特権 ID 管理 ・国民のためのサイバーセキュリティサイト　システムを“管理”する人向けの対策 Ｐ24 アクセス制御・管理 ・組織における内部不正防止ガイドライン 第 5 版 P42～43 (６)システム管理者の権限管理

No	チェック項目	想定されるリスクの例	対策の例	対策に参考となる情報の例
7	**ネットワークを守るためにファイアウォールや侵入検知システムを使っていますか？**	不正なアクセスやウイルス感染を防げず、情報漏洩のリスクが高まります。	社内ネットワークの入口・出口で、不正な通信を防ぐ仕組みを導入するなど	・中小企業の情報セキュリティ対策ガイドライン第 3.1 版 P50～51 ①ネットワーク脅威・端末対策 ・サイバーセキュリティ経営ガイドライン 経済産業省 P21～22 指示５ サイバーセキュリティリスクに効果的に対応する仕組みの構築 ・国民のためのサイバーセキュリティサイト システムを“管理”する人向けの対策 P14～16 ウェブサイトにおけるセキュリティ対策
8	**社外から社内システムへ安全にアクセスするために VPN（Virtual Private Network。インターネット上に安全な通信経路を作りデータの盗聴や改ざんを防ぐ技術）を使用していますか？**	VPN を使わずに公衆 Wi-Fi などを利用すると、通信を盗聴されるリスクがあります。	従業員が社外からアクセスするときは VPN を使い、通信を暗号化するなど	・中小企業の情報セキュリティ対策ガイドライン第 3.1 版 P42～45 (4)テレワークの情報セキュリティ ・インターネットの安全・安心ハンドブック Ver 5.10 P115～116 2.10 まとめて暗号化する VPN
9	**端末の不審な動きを監視する仕組み（EDR（Endpoint Detection and Response））を導入していますか？**	端末がウイルスに感染しても気づかず、攻撃が拡大するリスクがあります。	端末の動作を監視し、不審な動きがあれば管理者に通知するなど	・中小企業の情報セキュリティ対策ガイドライン第 3.1 版 P51 EDR（Endpoint Detection and Response) ・インターネットの安全・安心ハンドブック Ver 5.10 P171 3 サイバーセキュリティお助け隊サービス ・組織における内部不正防止ガイドライン 第５版 P54～57 (13)ネットワーク利用のための安全管理
10	**定期的にシステムの脆弱性をチェックしていますか？**	脆弱性を放置すると、攻撃者に狙われやすくなります。	脆弱性診断ツールを使い、古いソフトウェアや設定ミスを確認するなど	・国民のためのサイバーセキュリティサイト システムを“管理”する人向けの対策 P6～7 ソフトウェアの最新化・脆弱性管理 P17 脆弱性診断・ペネトレーションテスト ・インターネットの安全・安心ハンドブック Ver 5.10 P135～138 １社内・社外のセキュリティを向上しよう
11	**Web サイトを狙った攻撃を防ぐために WAF（Web アプリケーションファイアウォール）を導入していますか？**	WAF がないと、攻撃者に Web サイトを乗っ取られたり、情報が盗まれるリスクがあります。	WAF を使い、不正なアクセスを自動でブロックするなど	・中小企業の情報セキュリティ対策ガイドライン第 3.1 版 P51 WAF（Web Application Firewall） ・国民のためのサイバーセキュリティサイト システムを“管理”する人向けの対策 P14～16 ウェブサイトにおけるセキュリティ対策
12	**メールに添付されたファイルを検査し、危険なものをブロックしていますか？**	ウイルス付きの添付ファイルを開くと、マルウェア感染のリスクが高まります。	メールの添付ファイルをウイルスチェックし、不審なものは開かないようにするなど	・中小企業の情報セキュリティ対策ガイドライン第 3.1 版 P51 ②コンテンツセキュリティ対策 ・国民のためのサイバーセキュリティサイト システムを“管理”する人向けの対策 P11～14 電子メールにおけるセキュリティ対策 ・インターネットの安全・安心ハンドブック Ver 5.10 P41 ６⑤メールの添付ファイルや本文中のリンクに注意しよう

No	チェック項目	想定されるリスクの例	対策の例	対策に参考となる情報の例
13	**インターネットのアクセスを管理し、危険なサイトをブロックしていますか？**	危険なサイトにアクセスすると、ウイルス感染や情報漏洩のリスクがあります。	業務に関係のないサイトや危険なサイトへのアクセスを制限するなど	・中小企業の情報セキュリティ対策ガイドライン第 3.1 版 P51 ②コンテンツセキュリティ対策 ・組織における内部不正防止ガイドライン 第 5 版 P54～57 (13)ネットワーク利用のための安全管理
14	**疑わしいファイルをサンドボックス環境で検査し、安全性を確認していますか？**	ファイルの安全性を事前に確認しないと、未知のウイルスに感染するリスクがあります。	不審なファイルを仮想環境で実行し、リスクを事前に確認するなど	・国民のためのサイバーセキュリティサイト システムを“管理”する人向けの対策 P11～14 電子メールにおけるセキュリティ対策
15	**重要なデータを暗号化し、不正アクセスを防いでいますか？**	暗号化されていないと、情報が盗まれた際にそのまま悪用される可能性があります。	機密データを暗号化し、パスワードなしでは読めないようにするなど	・中小企業の情報セキュリティ対策ガイドライン第 3.1 版 P53 ⑤暗号化 ・国民のためのサイバーセキュリティサイト システムを“管理”する人向けの対策 P21 【コラム】UEFI のパスワードとハードディスク・SSD の暗号化 ・組織における内部不正防止ガイドライン 第 5 版 P58～59 (14)重要情報の受渡し保護 P60 (15)情報機器や記録媒体の持ち出しの保護 P61 (16)組織外部での業務における重要情報の保護
16	**不要なデータを適切に削除し、情報漏洩を防いでいますか？**	データを完全に消去しないと、削除したはずの情報が漏れるリスクがあります。	機密データを削除するときは、復元できない方法で処理するなど	・国民のためのサイバーセキュリティサイト システムを“管理”する人向けの対策 P4～5 安全なデータ・端末の廃棄 ・組織における内部不正防止ガイドライン 第 5 版 P47～48 (9)情報機器及び記録媒体の資産管理及び物理的な保護
17	**機密データの持ち出しを監視し、情報漏洩を防いでいますか？**	重要なデータが外部に持ち出されると、情報漏洩のリスクがあります。	DLP（データ漏洩防止）システムを使い、不審なデータの持ち出しを制限するなど	・国民のためのサイバーセキュリティサイト システムを“管理”する人向けの対策 P19～20 テレワーク時のルール策定 ・組織における内部不正防止ガイドライン 第 5 版 P49 (10)情報機器及び記録媒体の持出管理
18	**定期的にセキュリティインシデント対応訓練を行っていますか？**	事前に訓練しないと、実際に問題が起きたときに適切な対応ができず、被害が拡大する可能性があります。	インシデント対応の流れを決め、実際の訓練を行うなど	・中小企業の情報セキュリティ対策ガイドライン第 3.1 版 P46～47 (5)セキュリティインシデント対応 ・サイバーセキュリティ経営ガイドライン 経済産業省 P25～28 3．3 .インシデント発生に備えた体制構築
19	**DDoS 攻撃（大量のアクセスによるサーバーダウン）を防ぐ対策を導入していますか？**	DDoS 攻撃を受けると、Web サイトや業務システムが使えなくなり、業務に支障をきたす可能性があります。	DDoS 対策サービスを利用し、異常なアクセスを自動で検知・遮断するなど	・インターネットの安全・安心ハンドブック Ver 5.10 P159 7.9 DDoS 攻撃
20	**外部からの攻撃に備えて、定期的にペネトレーションテスト（システムの脆弱性を疑似攻撃で検査する手法）を実施していますか？**	事前に脆弱性を見つけて対策しないと、実際に攻撃を受けた際に被害が大きくなる可能性があります。	専門事業者やツールを活用し、実際の攻撃を想定した疑似的な攻撃や不正侵入のテストを行うなど	・国民のためのサイバーセキュリティサイト システムを“管理”する人向けの対策 P17 脆弱性診断・ペネトレーションテスト

No	チェック項目	想定されるリスクの例	対策の例	対策に参考となる情報の例
21	**セキュリティ事故が起きたときの連絡体制を整えていますか？**	緊急時に適切な対応ができないと、被害が拡大し、信用を失うリスクがあります。	インシデント発生時の連絡フローを決め、連絡先を整理し、誰にどのように報告するか明確にするなど	・中小企業の情報セキュリティ対策ガイドライン第 3.1 版 P24～31 4 本格的に取り組む P46～47 (5)セキュリティインシデント対応 ・国民のためのサイバーセキュリティサイト システムを“管理”する人向けの対策 P31～32 インシデントレスポンス体制整備
22	**重要な場所（サーバールームなど）への入退室ログを記録・管理していますか？**	物理的な侵入があっても記録がないと、不正アクセスの原因を特定できず、対策が遅れるリスクがあります。	入退室の履歴を自動で記録し、定期的にチェックするなど	・組織における内部不正防止ガイドライン 第 5 版 P45～46 (8)物理的な保護と入退管理 P111 対策のヒントとなる Q&A9 ・サイバーセキュリティ経営ガイドライン 経済産業省 P50 (23)リスク対応（回避、低減、移転、保有）
23	**サーバールームや機密エリアのセキュリティを強化していますか？**	無許可の人物がサーバールームに入ると、機器の破壊や情報漏洩のリスクが高まります。	入退室管理を厳格にし、監視カメラを設置するなど	・組織における内部不正防止ガイドライン 第 5 版 P45 (8)物理的な保護と入退管理 P111 対策のヒントとなる Q&A9 ・サイバーセキュリティ経営ガイドライン 経済産業省 P50 (23)リスク対応（回避、低減、移転、保有）
24	**災害やサイバー攻撃などの緊急事態に備えて、IT システムの事業継続計画（BCP 対策）を策定し、運用していますか？**	緊急対応が遅れると、システム停止が長引き、事業継続が困難になります。復旧が遅れると、顧客や取引先の信頼を失うリスクがあります。	災害や障害を想定し、IT システムの復旧手順をまとめた BCP を作成する。定期的に訓練を行い、従業員が迅速に対応できるようにするなど	・中小企業の情報セキュリティ対策ガイドライン第 3.1 版 P46～47 (5)セキュリティインシデント対応 ・サイバーセキュリティ経営ガイドライン 経済産業省 P23～24 指示 6 PDCA サイクルによるサイバーセキュリティ対策の継続的改善 P25～28 3.3. インシデント発生に備えた体制構築 P51 (27)BCP(Business Continuity Plan) ・インターネットの安全・安心ハンドブック Ver 5.10 P73 2.3 災害時の SNS での情報発信 P139～141 2 災害時やサイバー攻撃時に会社を守るために事業継続計画(BCP)を作ろう

※チェックリスト補足（業種別の活用ポイント）

以下に各業種における推奨されるセキュリティ対策の考え方を記載していますので、チェック時の参考としてください。

業種	推奨されるセキュリティ対策の考え方
鉄道	運行管理システムや駅設備の運用において、セキュリティリスクを考慮することが重要です。外部からの攻撃やシステム障害を想定し、適切な防御策を検討することが求められます。また、サプライチェーンを通じたリスクも想定されるため、取引先のセキュリティ状況を確認することが有効です。
バス	予約システムや運行管理システムを利用している場合、不正アクセスや情報漏洩を防ぐための管理が必要です。例えば、適切なアクセス制御や定期的なセキュリティチェックを実施することが対策の一つとなります。また、ウェブサイトの改ざんや不正利用を防ぐための対策を検討することも有効です。
バスターミナル	顧客情報を扱う場合、セキュリティリスクを考慮した情報管理の仕組みを整備することが重要です。不審なアクセスの監視や適切なネットワーク管理を行うことで、安全性の向上が期待できます。公共 Wi-Fi を提供する場合は、ネットワーク分離などの対策を検討することが適切です。
タクシー	配車アプリや決済システムを運用する場合、適切なアクセス管理を行うことが求められます。ドライバーが使用する端末のセキュリティ設定を適切に行い、紛失や不正アクセスのリスクを抑えることが重要です。
宿泊施設	予約管理システムや顧客データを安全に管理することが必要です。システムのバックアップを定期的に行うことで、ランサムウェアなどの攻撃に備えることが可能です。また、アクセス権限の管理を適切に行うことで、不正なデータ持ち出しを防ぐことができます。
フェリー・旅客船	予約システムや航行管理システムに関するリスクを考慮し、セキュリティ対策を実施することが求められます。取引先との連携を行う際には、サプライチェーンのセキュリティリスクを把握し、必要な対策を実施することが重要です。
空港・空港ビル	発券システムの安全性を維持するため、適切なセキュリティ対策を講じることが求められます。アクセス制御を強化し、不審な通信を検知する仕組みを導入することで、リスク低減につながります。公共 Wi-Fi を提供する場合は、ネットワーク分離などの対策を検討することが適切です。
航空	予約システムや運航管理システムを安全に運用するため、情報漏洩や不正アクセスに対する対策が必要です。ゼロトラストアーキテクチャの導入や多要素認証を利用することで、リスクを軽減することができます。
港湾	港湾管理システムや物流関連の情報システムに関して、不正アクセスや標的型攻撃を想定した対策が重要です。アクセス権限を適切に設定し、必要な人だけがデータにアクセスできるようにすることも有効です。
物流（倉庫）	在庫管理システムや配送管理システムを運用する場合、ランサムウェアの影響を最小限に抑えるための対策が必要です。定期的なバックアップの取得や、重要なデータの暗号化を行うことがリスク管理の一つの方法です。
物流（トラック）	輸送管理システムを活用する場合、外部からの不正アクセスや情報漏洩を防ぐための対策が求められます。不要なアカウントを削除し、アクセス管理を徹底することが有効です。また、取引先とのデータ連携を行う際には、セキュリティ基準の確認を行うことが望まれます。

業種	推奨されるセキュリティ対策の考え方
物流（海運）	貨物管理システムや船舶運航システムが標的型攻撃の対象となる可能性があるため、適切なセキュリティ対策を検討することが求められます。取引先のセキュリティ状況を評価することも有効です。
上水道	サイバーセキュリティに係る水道施設の技術的基準に適合することが求められます。また、制御システムがサイバー攻撃を受けた場合の影響を考慮し、ネットワーク分離や異常検知の仕組みを導入することが有効です。

※チェックリスト補足（リスク例の説明）

■ランサムウェア

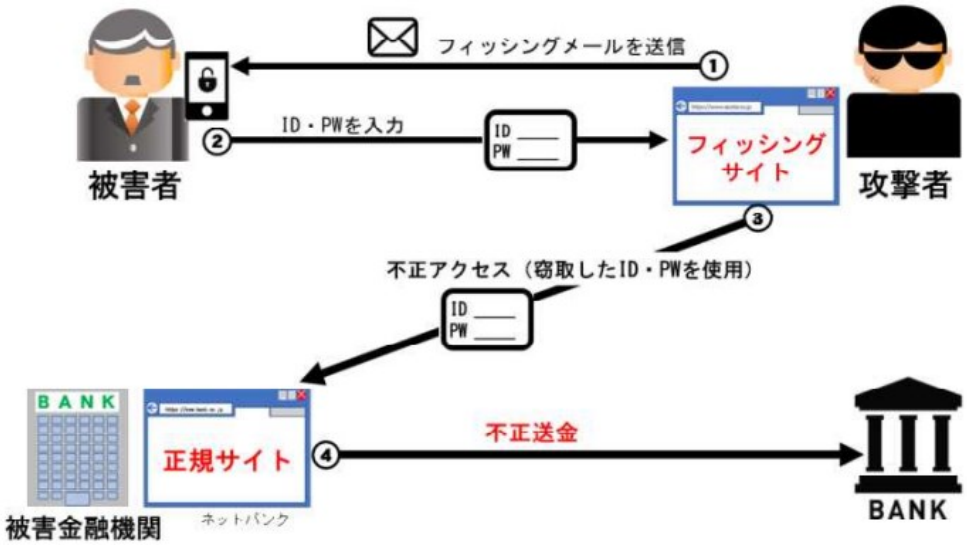
【出典】令和６年上半期におけるサイバー空間をめぐる脅威の情勢等について（警察庁）

ランサムウェアは、パソコンやサーバーのデータを暗号化し、使用できない状態にした上で、復旧のための身代金を要求するマルウェアです。感染すると業務に必要なデータが開けなくなり、業務の継続が困難になることがあります。

主な感染経路は、不審なメールの添付ファイルやリンクのクリック、脆弱なシステムへの攻撃、危険な Web サイトの閲覧などです。また、ネットワーク内で他の端末へ拡散するタイプもあり、被害が広がる可能性があります。

感染すると、データの復旧が難しく、たとえ身代金を支払っても元に戻る保証はなく、支払ってはいけません。そのため、事前の対策が重要です。まず、重要なデータは定期的にバックアップし、ネットワークから切り離して保管します。次に、OS やソフトウェアを常に最新の状態に更新し、脆弱性を狙った攻撃を防ぎます。さらに、従業員に対し、不審なメールを開かない、不用意にリンクをクリックしないなどの教育を行うことも効果的です。

■フィッシング



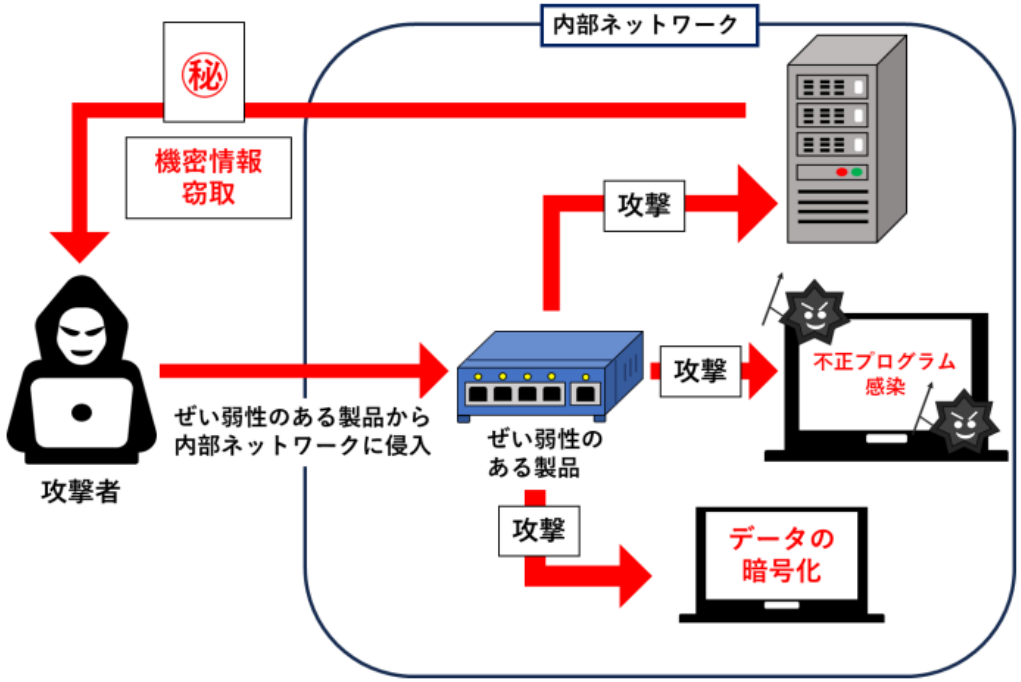
【出典】令和５年におけるサイバー空間をめぐる脅威の情勢等について(警察庁)

フィッシングとは、実在する企業や公的機関になりすましたメールや SMS を送り、偽のウェブサイト（フィッシングサイト）に誘導して個人情報を盗み取る詐欺の手口です。フィッシングサイトは本物のウェブサイトに酷似して作られており、そこで入力されたアカウント情報やクレジットカード番号が不正に取得されます。

盗まれた情報は、インターネットバンキングの不正送金やクレジットカードの不正利用に悪用されることが多く、企業や個人に大きな被害をもたらします。

対策として、不審なメールや SMS のリンクを安易にクリックせず、ログインが必要な場合は公式サイトから直接アクセスすることが重要です。また、メールの送信元や URL に不自然な点がないか確認し、二要素認証を設定することで被害を防ぐことができます。フィッシング詐欺は年々巧妙化しており、日頃から警戒を怠らないことが大切です。

■脆弱性に関する危険性



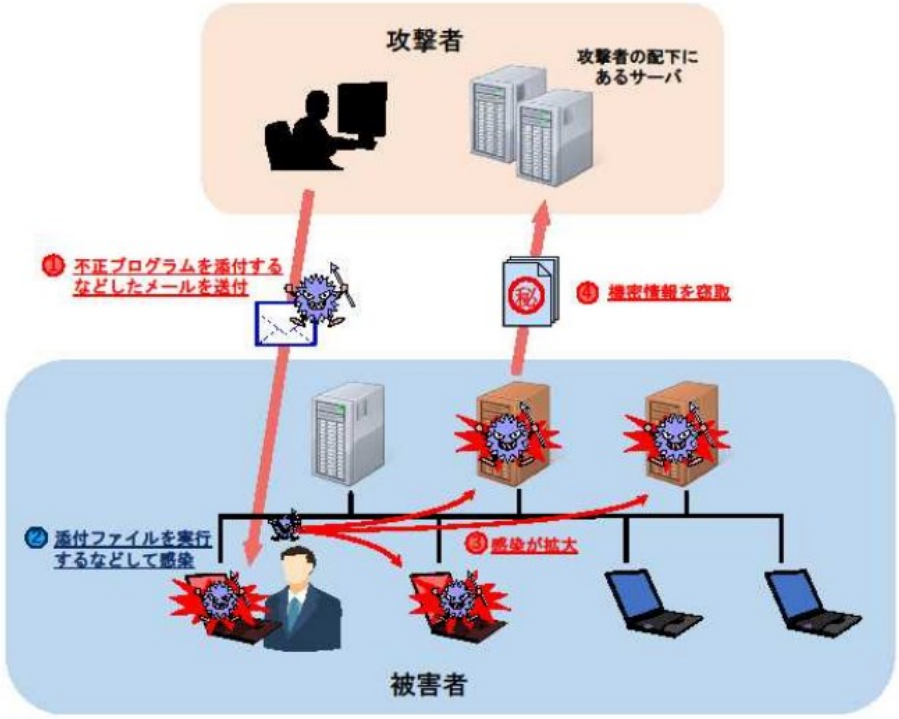
【出典】令和６年上半期におけるサイバー空間をめぐる脅威の情勢等について(警察庁)

脆弱性とは、システムやネットワーク機器に存在するセキュリティ上の弱点のことで、攻撃者は脆弱性を悪用して企業の内部ネットワークに侵入します。侵入された場合、不正プログラムの感染、機密情報の流出、ランサムウェアによるデータの暗号化など、さまざまなサイバー攻撃の被害を受ける可能性があります。

攻撃を受けると、被害拡大を防ぐためにシステムの運用を一時的に停止せざるを得なくなったり、重要な業務ファイルが暗号化されて使えなくなったりすることで、事業の継続に深刻な影響が及ぶことがあります。

このようなリスクを防ぐためには、OS やソフトウェアの更新のために、定期的にセキュリティパッチを適用することが重要です。また、不要な通信ポートを閉じる、アクセス制御を強化するなど、ネットワークの防御を強化することで攻撃のリスクを低減できます。企業のシステムが狙われることを前提に、日頃から脆弱性対策を徹底することが求められます。

■標的型攻撃



【出典】 令和５年におけるサイバー空間をめぐる脅威の情勢等について(警察庁)

標的型攻撃とは、特定の企業や個人を狙うために計画されたサイバー攻撃のことです。攻撃者は、実在する人物になりすましたメールを送り、相手と何度かやり取りを行うなどで信用させたうえで、不正なプログラム（マルウェア）を含むファイルを送付し、開かせる手口を使います。

また、メールの添付ファイルやリンクを利用し、フィッシングサイトへ誘導するケースもあります。攻撃者はターゲットが関心を持ちそうなファイル名をつけることで、警戒心を下げ、マルウェアを実行させようとすることもあります。

標的型攻撃は、一般的な迷惑メールとは異なり、ターゲットに合わせて内容が精巧に作り込まれているため、攻撃に気づきにくい特徴があります。対策として、不審なメールの添付ファイルやリンクを不用意に開かないことはもちろん、メール以外の手段を用いるなどで相手を慎重に確認することが重要です。また、セキュリティソフトの導入や従業員向けの教育を実施し、組織全体で警戒を強めることが求められます。

5 参考資料

本チェックリストにおける、セキュリティ対策の実施の参考となる資料をまとめています。

※参考資料リスト

No	資料名	作成元	URL
1	中小企業の情報セキュリティ対策ガイドライン	IPA （独立行政法人情報処理推進機構）	https://www.ipa.go.jp/security/guide/sme/about.html
2	サイバーセキュリティ経営ガイドライン	経済産業省	https://www.meti.go.jp/policy/netsecurity/mng_guide.html
3	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/
4	インターネットの安全・安心ハンドブック	NISC （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
5	組織における内部不正防止ガイドライン	IPA （独立行政法人情報処理推進機構）	https://www.ipa.go.jp/security/guide/insider.html
6	安全なウェブサイトの作り方	IPA （独立行政法人情報処理推進機構）	https://www.ipa.go.jp/security/vuln/websecurity/about.html
7	無線 LAN（Wi-Fi）の安全な利用（セキュリティ確保）について	総務省	https://www.soumu.go.jp/main_sosiki/cybersecurity/wi-fi/
8	テレワークにおけるセキュリティ確保	総務省	https://www.soumu.go.jp/main_sosiki/cybersecurity/telework/