情報漏えい！

1 ウィルス・マルウェアを水際で防ぐ！



・Webサイト、アプリ等の脆弱性を定期的に見直す。
・パターンファイルを常に最新のものに更新する。
・不審なメールは開かない、添付ファイルをDLしない、情報システム部門にすぐに連絡する。
・最新のサイバー攻撃の実態・手口を知る。

2 ソフトウェア更新で脆弱性を解消！



・OS、ブラウザ、アプリケーション、ファームウェアは常に最新版に更新する。
・自動更新を有効又は定期的にアップデートを確認する。
・日頃からソフトウェア開発元、メーカーの脆弱性に関するサポート情報や、国内外の脆弱性情報に関する調整機関の発表に関心を持ち、迅速な対応をとる。

3 不正アクセスを許さない！





・不正アクセス検知・警報装置を導入する。
・パスワードは複数のサービスで使い回さない。
・離席時はログアウト、パスワードを入力してログインする。
・多要素認証のうち、２つ以上を組み合わせた認証方法を導入する。
・アクセス権の付与対象者は最小化する。

4 万が一のインシデント対応！



・情報セキュリティポリシーを導入し継続的な運用を行う。
・怪しい挙動時は即時にネットワークから遮断する。
・BCP(事業継続計画)を策定し、インシデント発生時は速やかにCSIRTを立ち上げる。
・インシデント発生時は速やかに関係企業、警察へ連絡する。

5 利用者への注意喚起！



・不正アクセスされた企業を装ったフィッシングメールに注意する。
・クレジットカード情報の流出時は利用停止、再発行をする。
・住所、生年月日を利用したもの、使い回しのパスワードは変更をする。
・免許情報の流出は信用情報機関へ登録する

新潟県警察本部　サイバー犯罪対策課