サイバーセキュリティ基本方針について

2025 年 10 月 10 日
株式会社協栄ファスナー工業
代表取締役 松本 悠

1.基本理念

株式会社協栄ファスナー工業は、自動車をはじめとする社会の安全・安心を支える金属部品メーカー として、顧客取引先・社員など、すべての関係者の信頼を守ることを責務とし、情報資産を保護することを経営の基盤の一つと位置づけ、サイバー攻撃・情報漏えい・システム停止などのリスクから会社を守るため、全社員が一体となってサイバーセキュリティ対策に取り組みます。

2.サイバーセキュリティの目的

・お客様の信頼、自社の信頼を守ること
・生産・出荷の停止を防ぐこと
・機密情報(設計図・単価・顧客データ)の漏えい防止
・社員全員で「守る文化」をつくること

3. 脅威の具体例

脅威	⇒想定される影響
不審メール (マルウェア)	⇒工場システム停止、情報漏えい
USB や外部記録媒体	⇒ウイルス感染、データ流出
パスワード共有	⇒不正アクセス、情報改ざん
クラウド誤設定	⇒顧客データの漏えい
不審なサイト閲覧	⇒マルウェア感染、情報損失

4.組織体制と責任分担

■ 経営層(社長)
・サイバーセキュリティ基本方針の策定
・必要な予算と体制の整備
・インシデント発生時の最終判断・対外対応
■ 管理部門(営業・調達・生産・生管・品管・管理等各部署の管理者)
・社員教育・周知の企画と実施
・情報資産の分類と管理(顧客情報、契約データ等)
・外部委託先とのセキュリティ契約確認

インシデントとは
「出来事」「事件」という意味の英単語です。
それが転じて、情報セキュリティシーンでは
パスワードの漏洩や不正アクセス、
マルウェア感染など、コンピューターおよび
ネットワークのセキュリティ(安全性)を脅かす
事象として使用されています。

■ システム管理者(情報担当/デジタル化推進)
・社内ネットワーク・サーバ・端末の安全設定
・ウイルス対策・バックアップ・アクセス権設定
・ログ監視と退社・異動時の権限削除
・インシデント対応
・ソフトウェアの更新・パッチ適用管理
■ 製造・現場部門
・USB・外部機器の持ち込み禁止徹底
・ID・パスワードの管理徹底
・不審なメール・挙動の即時報告
・機密図面やデータの管理徹底、廃棄ルール遵守

4.インシデント対応フロー(例)

①不審メール・感染・異常を発見
②上長・システム管理者へ即時報告
③該当端末をネットワークから切断し、ウイルス対策ソフトでウイルスチェックを実施
④原因調査・影響範囲の特定
　(外部に協力依頼⇒島根県警サイバーセキュリティ対策係 TEL:0852-26-0110)
⑤経営層判断のもと、顧客・関係先へ連絡対応

5.教育と継続改善

・年１回以上の社内教育実施(全体朝礼、各部署での朝礼等)
・新入社員への初期教育
・外部監査や取引先監査への対応

6. 社員一人ひとりが意識すべき行動

・不審メールは開かない ・ リンクを押さない
・パスワードは使い回さない、管理を徹底する
・セキュリティは「自分ごと」として考える ・定期的なデータバックアップ

7. まとめ

「一人の油断が全体の停止に繋がる」
安全なものづくりのために、全員で守る意識を。

以上