最新の情報セキュリティ 2023

株式会社Purpom Media Lab

ISMS教育教材

doc_id: EDU-MAT-002 ／ version: 1.0
制定日: 2024年4月1日

1. 2023年の情報セキュリティ動向

近年、サイバー攻撃は高度化・組織化が進んでいます。特に中小企業や委託先を狙ったサプライチェーン攻撃が増加しています。

> **2023年に特に注目された脅威**
>
> - **ランサムウェア攻撃の増加**：データを暗号化し身代金を要求。医療機関・インフラへの攻撃が多発
> - **フィッシング詐欺の巧妙化**：実在する企業・上司を装ったメールが増加
> - **クラウドサービスの設定ミス**：S3バケット等の公開設定ミスによる情報漏えい
> - **サプライチェーン攻撃**：取引先・委託先を経由した標的型攻撃

2. ランサムウェアへの対策

ランサムウェアは一度感染すると復旧が困難で、事業継続に深刻な影響を与えます。

感染経路

- 不審なメールの添付ファイル・URLのクリック
- リモートデスクトップの脆弱性悪用
- ソフトウェアの脆弱性（未パッチ）

> **対策**
>
> - OSやソフトウェアを常に最新の状態に保つ
> - 重要データの定期バックアップ（クラウドへの自動バックアップ推奨）
> - 不審なメールは開かず、IT担当者に報告する

3. フィッシング詐欺の見分け方

確認ポイント	詳細
送信元メールアドレス	ドメインが公式と異なる（例: amazon-support@gmail.com）
リンク先URL	ホバーして表示されるURLが公式ドメインと異なる
文章の不自然さ	日本語が不自然、緊急を煽る表現
添付ファイル	心当たりのない請求書・契約書等

4. クラウドサービスの安全な利用

当社ではGoogleドライブを情報共有の標準ツールとして採用しています。

> **Googleドライブ利用時の注意点**
>
> - 共有設定は「特定のユーザー」のみ。「リンクを知っている全員」は原則禁止
> - 外部共有が必要な場合はISMS担当者に確認

- 退職者・業務終了した委託先のアクセス権は速やかに削除

5. パスワード管理の最新ベストプラクティス

- 12文字以上、英数字記号を組み合わせる
- サービスごとに異なるパスワードを使用（パスワードマネージャー推奨）
- 多要素認証（2FA）を必ず有効化する
- 定期変更よりも「漏えい時の即時変更」を優先

受講確認
本教材の内容を理解し、最新の脅威動向を踏まえた適切な行動をとることを確認しました。