CyberCrime Control Project

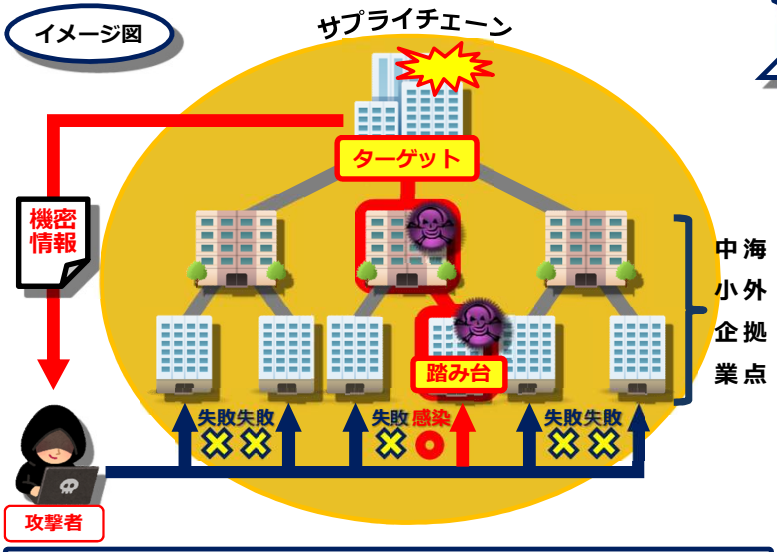
令和２年 第３号

広島県警察本部
サイバー犯罪対策課
082-228-0110
（内線　705-586）

ー サプライチェーン攻撃が増加しています ー

サプライチェーン攻撃とは、企業活動におけるサプライチェーン（供給網）につけ込む攻撃のことです。
ターゲットとなる企業（大企業）を直接狙うのではなく、**取引先企業（中小企業等）を踏み台**にして攻撃します。

イメージ図



大企業に比べて、セキュリティが比較的に弱い中小企業や海外拠点などが狙われ、**踏み台**として利用されます。

侵入経路確立手段

侵入経路を確立するために、あらゆる手段で攻撃してきます！

以下のような手段で侵入経路を確立しています。

メール

- 委託先・委託元を乗っ取り、なりすましメールを送付
- 請求書支払い等を装ったなりすましメールを送付

納品物

- 委託先からの納品物にウィルスが混入
- 調達したソフトウェア・オープンソースソフトウェアの脆弱性を突く

引用　経済産業省　https://www.meti.go.jp/press/2020061204/20200612004-1.pdf
　　Ｉ　Ｐ　Ａ　https://www.ipa.go.jp/files/000073868.pdf

基本的な対策　ーまずはここから始めましょう！ー

Check!　**令和２年６月12日に経済産業省からも取り組みの方向性が掲示されました！**
経済産業省（ＵＲＬ）https://www.meti.go.jp/press/2020/06/20200612004/20200612004.html

＜重要情報の特定＞

情報の把握・整理が重要です！

- ○ 重要情報と一般情報に分けて管理（情報の格付け区分）
- ○ 重要度ごとに取扱いルールを定め、定期的に見直す（取扱範囲、廃却方法等）
- ○ 従業員にわかるように「情報区分」を表示（ラベル付け）

引用　ＩＰＡ　https://www.ipa.go.jp/files/000073868.pdf

接近の制御

- ○ 情報の重要度によって分けて保管する
- ○ 重要度の高い情報の保管場所に入場制限を設ける
- ○ ファイルにアクセス権及びパスワードの設定
- ○ ファイアウォール等の導入
- ○ ウイルス対策ソフトの導入

持出しの困難化

- ○ 業務用資料のコピー制御
- ○ パソコンを持ち出すことができないようにする
- ○ パソコンのローカルドライブに業務用資料のコピーを制御する
- ○ ＵＳＢメモリ等を利用した複製の制御

視認性の確保

- ○ 防犯カメラの設置
- ○ 「立ち入り禁止」等の張り紙等の設置
- ○ 社員証等の着用の義務付け
- ○ 座席配置等のレイアウトを工夫する
- ○ 保管場所等の整理整頓

引用　ＩＰＡ　https://www.ipa.go.jp/files/000073868.pdf

サイバーセキュリティ対策５か条

1. 不審なメールは開かない
2. 大切なデータは必ずバックアップ（Back up!）
3. ＯＳやソフトウェアは必ずアップデート（最新）
4. ソフトやアプリは信頼できる場所からダウンロードする（公式）
5. パスワードは使い回しをしない（Pass word）

平成 28 年～令和２年
「めざそう！安全・安心・日本一」
ひろしまアクション・プラン

運動目標　県民だれもが穏やかで幸せな暮らしを実感できる
日本一安全・安心な広島県の実現

重点項目
- 身近な犯罪被害の抑止
- 子供・女性・高齢者等の安全確保
- 新たな犯罪脅威への対応

なくそう特殊詐欺被害　アンダー５作戦
なくそう交通死亡事故　アンダー75作戦