令和5年9月28日発行

# 静岡県警察からのお知らせ

## 「BlackTech」による攻撃に注意！

### 【BlackTechとは】

中国を背景とするサイバー攻撃グループで、日本を始めとする各国の政府、産業、技術、メディア、エレクトロニクス及び電機通信分野を標的とし、情報窃取を目的としたサイバー攻撃を行っています。

ネットワーク機器やソフトウェアの脆弱性を狙うほか、各種機器の設定不備、サポート切れの製品の脆弱性など様々な攻撃を仕掛けてきます。

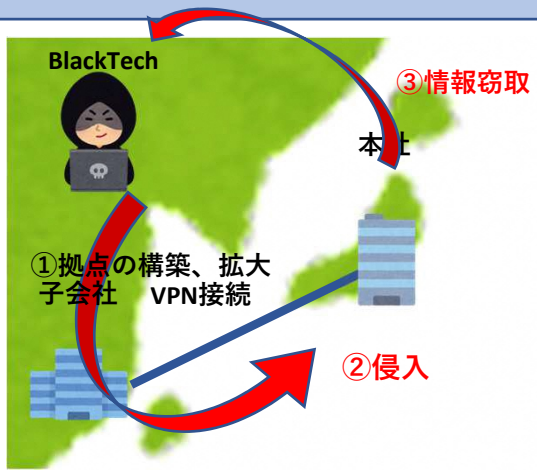
### 【子会社からの侵入】

① 子会社に侵害拠点を構築し、侵害活動を拡大

② 本社との接続用ネットワーク機器を通じて、本社に侵入

③ 情報窃取

※ **すでに自組織だけでなく、関連グループ組織、システムの開発・保守業者等が侵害を受けている可能性があることを念頭にこれら関連グループ等と連携して対策する。**




### 【リスク低減の対処例】

① ネットワーク機器やソフトウェアの**修正パッチの迅速な適用**

② **端末の保護**（EDRやウイルス対策ソフトの導入）

③ **不要なソフトウェアの排除**、**ネットワークの分割**

④ **本人認証の強化**（複雑なパスワード）、**多要素認証の実装**

⑤ アカウント等の**権限の適切な管理・運用**

⑥ **侵害の継続的な監視**（各種ログの保存・確認）

⑦ **インシデント対応計画**、**システム復旧計画の作成**

⑧ **完璧な防御はできないと考えて対策**をする（ゼロトラスト）

### 【被害発生時】

所管官庁への報告とともに、
**警察への通報**をお願いします。

**通報を受けて警察では**
- **被害拡大防止**
- **攻撃者追跡のための証拠保全**
- **復旧に向けた助言**

**などを行います**

**警察庁公表の詳細版はこちら**

https://www.npa.go.jp/bureau/cyber/pdf/20230927press.pdf


発行 静岡県警察本部生活安全部サイバー犯罪対策課サイバーセキュリティ対策係
TEL(代表)054－271－0110 (内線)711－3482


警察庁 National Police Agency