



静岡県警察からのお知らせ

サイバー空間の脅威の情勢：極めて深刻

1 我が国に対するサイバー攻撃が複数発生！

DDoS攻撃によるとみられるウェブサイトの閲覧障害が複数発生
 一部の事案に関しSNS上でハクティビスト（※）や親ロシア派ハッカー集団からの
 犯行をほめかす投稿を確認 ※ 社会的・政治的な主義主張を目的としたハッキング活動を行う者

2 ネットバンクの不正送金被害の発生件数が過去最多！

【情勢】

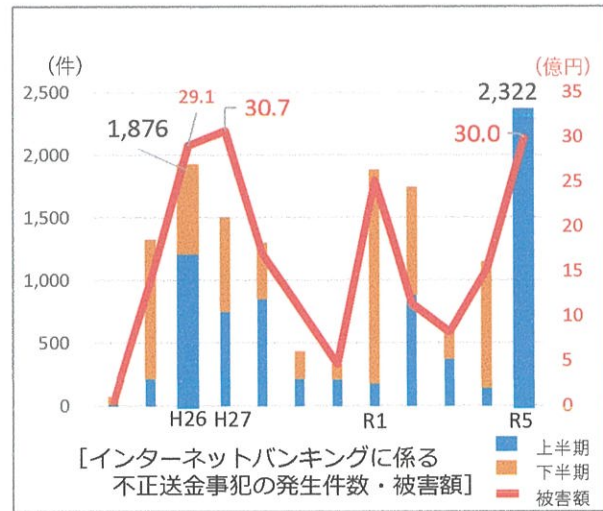
- インターネットバンキングに係る不正送金被害は、発生件数2,322件、被害総額約30億円
- 年間の数字と比較しても、発生件数は既に過去最多、被害額も過去最多に迫る勢い

【対策（個人向け）】

- メール等のリンクは安易にクリックしない
- 公式アプリ、公式サイトを利用する

【対策（企業向け）】

- なりすましメール対策技術（SPF・DKIM・DMARC）を導入する
- 利用状況通知サービスを導入する 等



静岡県内においても、発生件数47件、被害総額約1.3億円と被害額は過去最多、被害件数も過去最多（年間50件）に迫る勢い（詳細は令和5年8月9日発行の静岡県警察からのお知らせ）

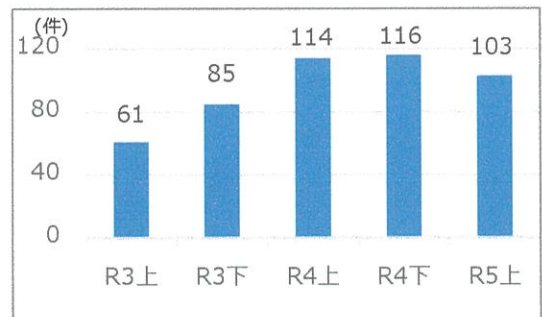
3 ランサムウェアの感染被害が高水準で推移！

【情勢】

- ランサムウェア被害は103件で、高水準で推移
- ランサムウェアによる被害のほか、データを暗号化することなくデータを窃取し対価を要求する手口（「ノーウェアランサム」）による被害が、新たに6件確認

【対策】

- 機器等にパッチ等を適用する（ぜい弱性対策）
- バックアップデータをオフラインで保管する



【ランサムウェアの被害の報告件数】

警察庁公表の詳細版はこちら



https://www.npa.go.jp/publications/statistics/cybersecurity/data/R05_kami_cyber_jousei.pdf



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】

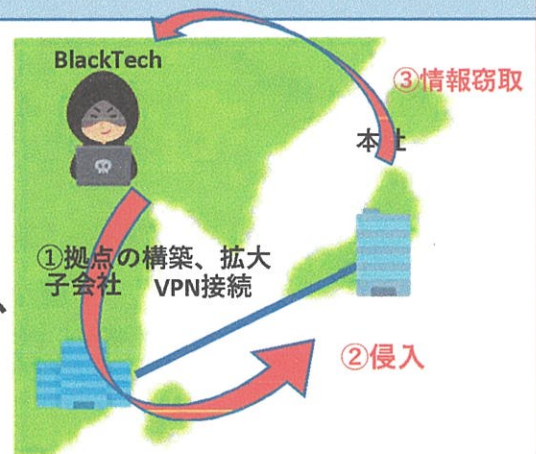
中国を背景とするサイバー攻撃グループで、日本を始めとする各国の政府、産業、技術、メディア、エレクトロニクス及び電機通信分野を標的とし、**情報窃取**を目的としたサイバー攻撃を行っています。

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