令和６年におけるサイバー空間をめぐる脅威の情勢について

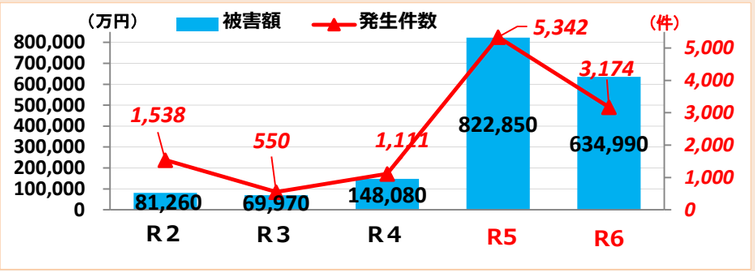
令和７年４月１１日
サイバーセキュリティ対策本部

インターネットバンキングに係る不正送金事犯（都内）

◆ 発生件数　３，１７４件
（前年比　－２，１６８件）
◆ 被害額　約63億4,990万円
（前年比　－約19億1,760万円）

令和５年と比較して、発生件数が約41%減少し、被害額も約23%減少した。
手口の9割はフィッシングによるものだった。

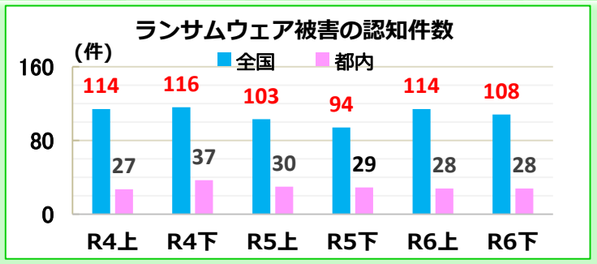
発生件数・被害額



※　各金融機関が推奨するセキュリティ対策を積極的に活用しましょう。
※　メールやSMSに記載されたリンクはクリックせず、内容の確認は、公式サイトやアプリを利用しましょう。
※　携帯電話会社等の迷惑メッセージブロック機能を活用しましょう。
※　公式サイト以外からのソフトやアプリのダウンロードは、ウイルスに感染する危険があります。
ダウンロードは、信頼できるサイトから行いましょう。
※　パスワードの使い回しは危険です。複雑で強力なパスワードを設定し、管理しましょう。

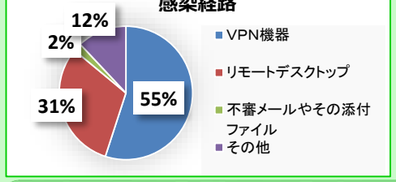
ランサムウェアの情勢

◆ ランサムウェア被害の特徴
・　令和６年においても、被害は高水準で推移している。
・　感染経路は、VPNとリモートデスクトップが大半で全体の86%を占めている。
・　バックアップを取っていても、ネットワーク上に保存していたため、暗号化されて復元できなかったケースが73%と多い。

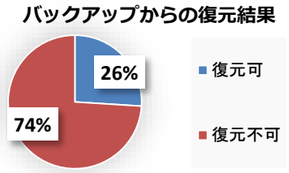


◆ 警察庁が実施した全国でランサムウェア被害に遭った企業・団体等に対するアンケート調査回答の分析結果

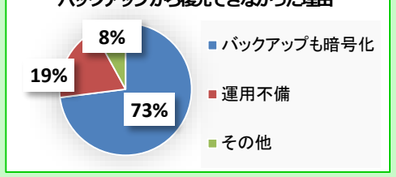
感染経路



バックアップからの復元結果



バックアップから復元できなかった理由



※　ＯＳやアプリケーション、ＶＰＮ機器等は常に最新の状態にアップデートし、セキュリティソフトを導入しましょう。
※　複雑で強力なパスワードを設定し、アカウントの管理を徹底しましょう。
※　バックアップはネットワークから物理的に切り離して保管しましょう。

サイバー攻撃の情勢

情　勢

★ 当庁把握のサイバー攻撃手法について
令和６年中、当庁で把握したサイバー攻撃手法は、ネットワーク機器やＯＳの脆弱性を突く攻撃が多くみられた。
また、社会的影響をもたらすＤＤｏＳ攻撃も相次いで発生した。

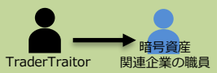
★ 重要インフラ事業者に対するウェブサイト等の閲覧障害
12月下旬から翌年1月上旬にかけ、交通機関や金融機関等の重要インフラ事業者において、DDoS攻撃による被害とみられるウェブサイトの閲覧障害や各種サービスへのアクセス障害が発生した。

★ MirrorFaceによるサイバー攻撃に関する注意喚起
令和７年1月、警察庁は、当庁及びサイバー特別捜査部ほか道府県警察による捜査の結果を踏まえ、中国の関与が疑われるMirrorFaceと呼称されるサイバー攻撃グループが、我が国の安全保障や先端技術に係る情報窃取を目的とした、組織的なサイバー攻撃を行っていることを確認した。そこで同グループによるサイバー攻撃の手口や未然防止対策等に関する注意喚起を実施した。

当　庁　の　取　組

★ TraderTraitorに対するパブリック・アトリビューション
5月、暗号資産関連企業の職員にリクルーターになりすまして接触し、必要な情報を窃取するソーシャルエンジニアリングの手法を用いた暗号資産(約482億円相当)の窃取事案が発生した。
12月、警察庁は、当庁及び関東管区警察局サイバー特別捜査部による分析結果を総合的に評価し、米国連邦捜査局（ＦＢＩ）及び米国国防省サイバー犯罪センター(ＤＣ３)とともに、同事案は北朝鮮を背景とするサイバー攻撃グループ「TraderTraitor」によるものであることを特定し、合同で文書を発出した。

ソーシャルエンジニアリング（TraderTraitorの手口）



リクルーターになりすましSNSを通じて標的に接触し、騙された標的をマルウェアに感染させるよう誘導した。

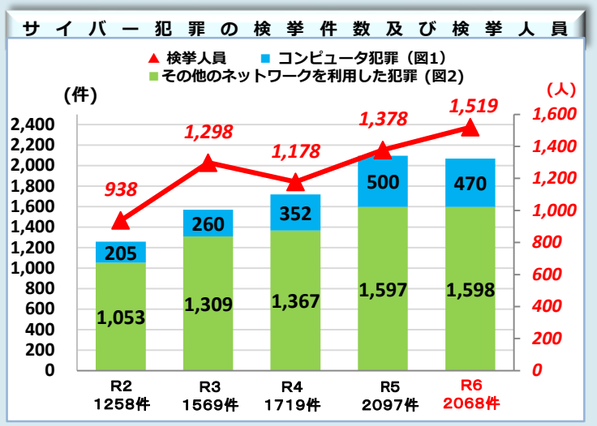
サイバー犯罪の検挙状況（都内）

◆ 検挙件数　２，０６８件（前年比　－２９件）
◆ 検挙人員　１，５１９人（前年比　＋１４１人）

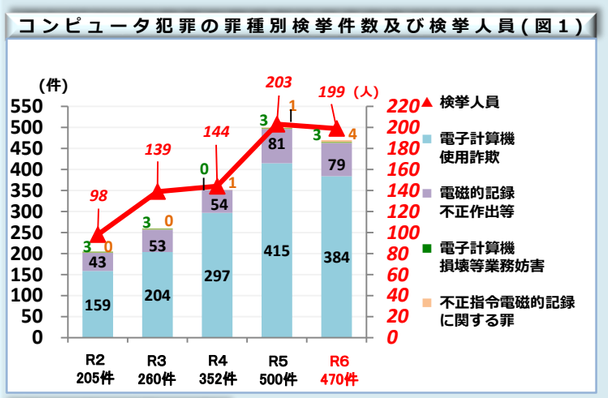
検挙件数は、昨年に引き続き高水準で推移しており検挙人員は昨年比で約10%増加した。
罪種別検挙件数の内訳では、昨年に引き続き、コンピュータ犯罪の電子計算機使用詐欺の検挙及びその他ネットワークを利用した犯罪の詐欺の検挙がそれぞれ最も多く、その内容は、いずれも特殊詐欺関連事件のものが多かった。

※本統計の数値は、各所属からの報告に基づく手集計による。

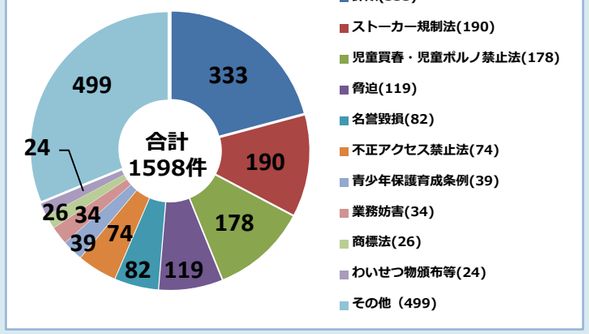
サイバー犯罪の検挙件数及び検挙人員



コンピュータ犯罪の罪種別検挙件数及び検挙人員（図１）



その他のネットワークを利用した犯罪の罪種別検挙件数の内訳(図2)



検　挙　事　例

【少年によるSNSを利用した暗号資産無登録交換業事件】
3月、内閣総理大臣の登録を受けないで、業として、交換依頼者である高校生Aほか1名から暗号資産を購入した上、交換依頼者である会社員Bに暗号資産を売却した少年を資金決済に関わる法律違反で検挙した。

【生成ＡＩを利用した不正指令電磁的記録作成事件】
５月、生成ＡＩを利用して、電子計算機上のデータを上書きして破壊する機能を有するソースコードを作成した無職の男を不正指令電磁的記録に関する罪（不正指令電磁的記録作成等）で検挙した。

都民・企業等に向けた取組

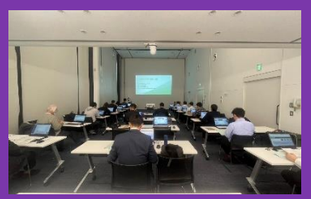
都　民　に　向　け　た　取　組

★　都内全域において、高齢者を含む幅広い世代に対し啓発リーフレット等を配布する街頭キャンペーンやスマホ防犯教室等を実施した。

スマホ防犯教室

中　小　企　業　に　向　け　た　取　組

★　区市町村との協定を活用し、都内全域において、中小企業のニーズに応えたサイバーセキュリティセミナーを実施した。



サイバーセキュリティセミナー

重要インフラ事業者等に向けた取組

★　重要インフラ事業者や先端技術保有事業者等を対象とした対処訓練を実施するなど、サイバー攻撃に対する対処能力向上を図った。

官民共同対処訓練