第５　サイバー空間の安全の確保と警察活動

１　社会全体の意識の向上に向けた取組

(1)　産学官連携によるサイバーセキュリティ対策

サイバー空間の安全を確保するためには、産業界・学術機関・官公庁と連携した取組が重要です。

北海道警察では、「北海道地域情報セキュリティ連絡会」（Hokkaido Area Information Security Liaison、通称：HAISL）の運営等を通じて各業界と情報共有を行うとともに、連絡会やセキュリティセミナー等を開催してサイバーセキュリティ意識の向上を図っています。

また、HAISLでは、次代を担うサイバーセキュリティ人材の育成のため、学生がサイバー空間の正しい利用方法やセキュリティ対策について学ぶ場である「Security College for Youth」（通称：SC4Y）を立ち上げ、勉強会やセキュリティ競技会を開催しています。

【ＨＡＩＳＬ】

【セキュリティセミナー】

【SC4Y勉強会】

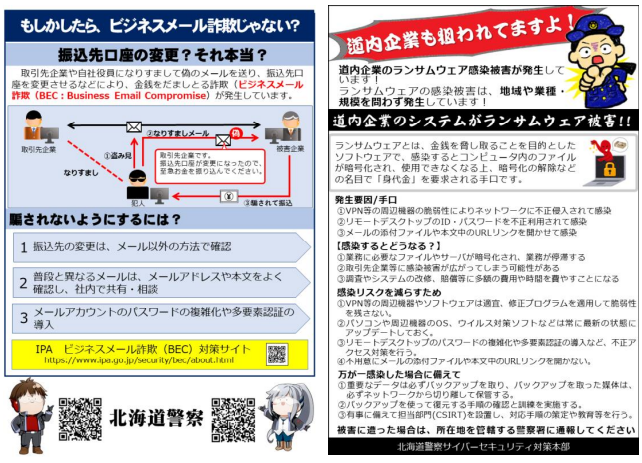
(2)　事業者等に対するサイバーセキュリティ対策

道内の経済を担って活躍している事業者・団体が、サイバー犯罪の被害やサイバー攻撃に遭った場合、その被害は当該事業者等に止まらず、一気に拡散し、道民生活全体に悪影響を及ぼす事態となることも考えられます。

北海道警察では、道内で大多数を占める中小事業者のサイバーセキュリティ対策の向上を図るため、商工団体等で構成する「北海道中小企業サイバーセキュリティ支援ネットワーク」（通称：Cyber-道net）を設立・運営し、サイバー犯罪の最新情勢やセキュリティ面のぜい弱性等に関する情報をタイムリーに発信しています。

また、セキュリティセミナー等の開催、出前講話の実施など、事業者等のサイバーセキュリティ対策の向上に向けた各種取組を推進しています。

【Cyber-道netサイバーセキュリティ演習】



【事業者向け広報資料】

(3)　道民に対するサイバーセキュリティ対策

「サイバー空間の脅威」に関する正しい知識と対処能力を身に付けてもらえるよう、最新のサイバー情勢を反映した広報資料を作成の上、ネットワーク等を通じて広く道民に情報発信しているほか、イベントや出前講話等の機会において、サイバーセキュリティに関する広報啓発活動を行っています。

【大学における講話】

【一般向け広報資料】

【児童・生徒・学生向け広報資料】

また、専門学校と連携してYouTube動画や啓発ポスターを制作したり、プロバスケットボールクラブ「レバンガ北海道」にサイバーセキュリティアンバサダーを委嘱して協働した広報啓発活動を展開するなど、幅広い世代に対して注意喚起を実施しています。

【ポスター】

【YouTube動画】

【アンバサダー委嘱式】

【選手が参加した啓発活動】

２　警察の対処能力の向上に向けた取組

職員のサイバー事案対処能力の向上や専門的知識を有する捜査員の育成のため、警察学校に入校した職員に対してサイバーセキュリティ教養を実施しています。

そのほかに警察本部・方面本部の各所属と各警察署に対する教養やインターネットを使用した実戦的なサイバー捜査に関する教養を実施し、対処能力の向上に向けた人材育成を推進しています。

【部外講師によるサイバー捜査セミナー】

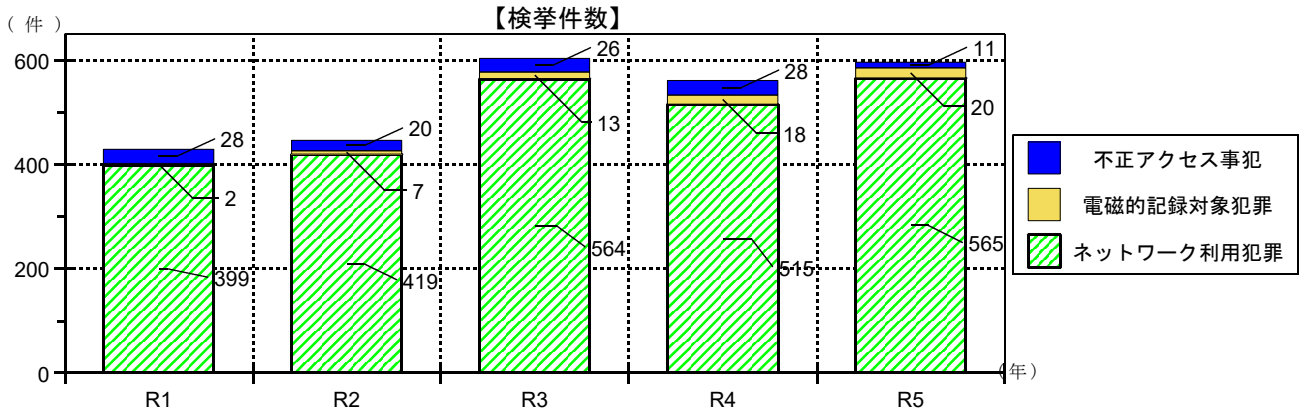
【サイバー捜査演習】

３　サイバー犯罪の取締りと対策

(1)　サイバー犯罪の現状

サイバー犯罪には、パスワードなどで保護された他人のコンピュータに無断でアクセスする「不正アクセス事犯」、他人のコンピュータのデータを破壊・改ざんしたり、コンピュータウイルスに感染させるなどの「電磁的記録対象犯罪」、電子掲示板やファイル共有ソフトを利用して違法な画像・動画等を公開したり、メールやＳＮＳを利用して他人を脅迫するなどの「ネットワーク利用犯罪」があります。

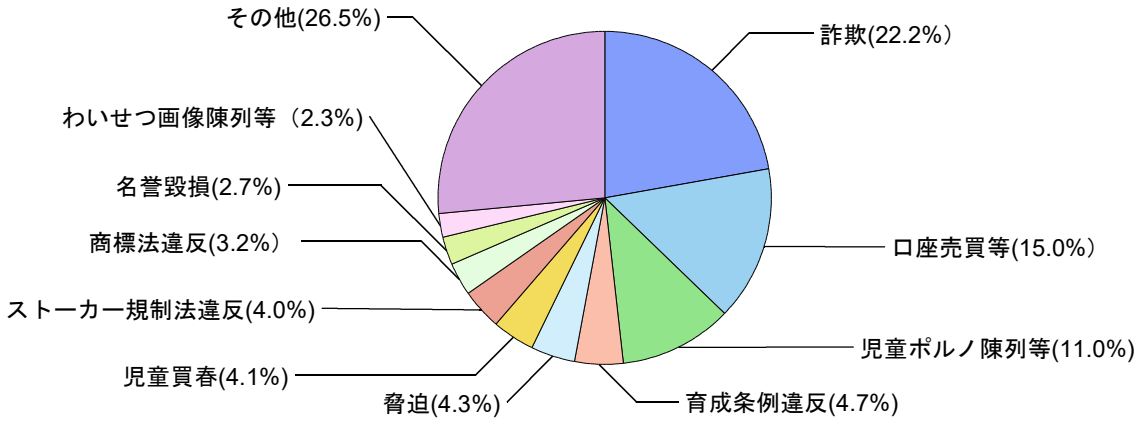
令和５年中、北海道警察では596件のサイバー犯罪を検挙しました。



(2)　ネットワーク利用犯罪の検挙罪種の割合

令和５年中、北海道警察で検挙したネットワーク利用犯罪は、コロナ関連持続化給付金等の詐欺事件の割合が22.2％で全体の約５分の１、子どもの性被害に関係する児童買春、児童ポルノ、北海道青少年健全育成条例違反事件の割合が19.8％で全体の約５分の１を占めました。

【ネットワーク利用犯罪検挙罪種割合（令和５年：北海道内）】



(3)　令和５年中の主な検挙事例

《事例》

令和５年11月、来店客のアカウントに不正アクセスし、現金相当のポイントを不正に自己のアカウントに送金した元店舗従業員の女を、不正アクセス禁止法違反、私電磁記録不正作出・同供用、電子計算機使用詐欺罪で検挙しました。

（浦河署、サイバー犯罪対策課）

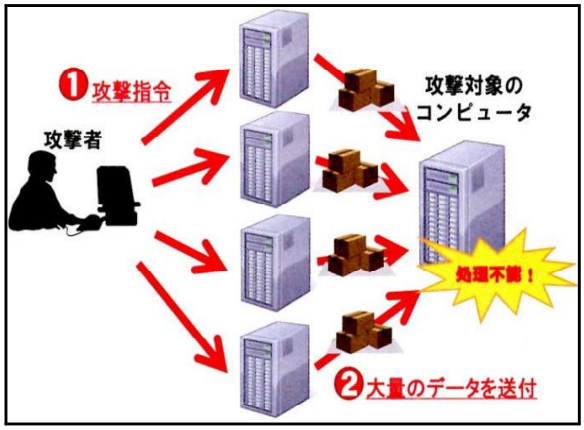
4　サイバー攻撃対策

(1)　サイバー攻撃の現状

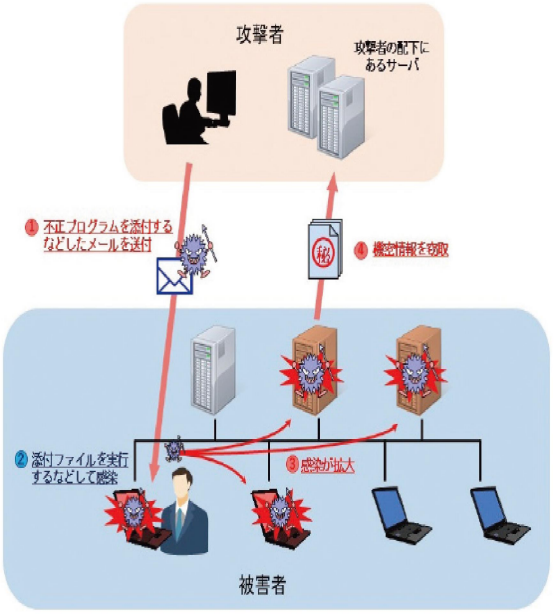
ア　サイバー攻撃情勢

インターネットが国民生活や社会活動に不可欠な社会基盤として定着し、サイバー空間は国民の日常生活の一部となっています。こうした中、重要インフラの基幹システムを機能不全に陥れ、社会の機能を麻痺（まひ）させてしまうサイバーテロや情報通信技術を用いて政府機関や企業等から機密情報を窃取するサイバーインテリジェンスといったサイバー攻撃は、国の治安、安全保障及び危機管理にとって現実の脅威となっています。

サイバー攻撃には、①攻撃の実行者の特定が難しい、②攻撃の被害が潜在化する傾向がある、③国境を容易に越えて実行可能であるといった特徴があり、我が国においても、サイバー空間の脅威に対する対処能力の強化が求められています。



【ＤＤｏＳ（ディードス）攻撃】

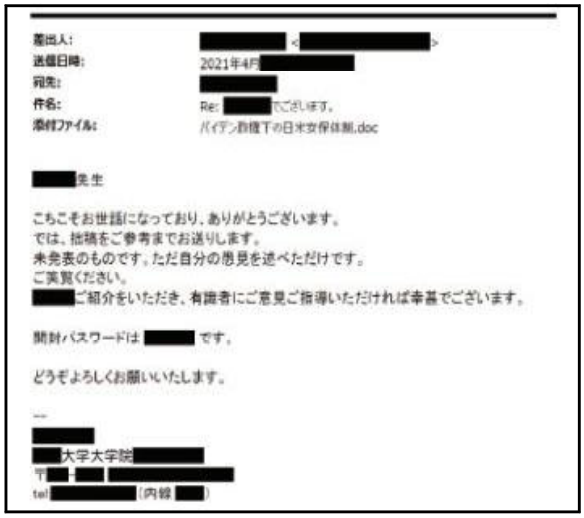


【標的型メール攻撃による情報窃取の例】

イ　サイバー攻撃の手口

サイバー攻撃の手口としては、攻撃対象のコンピュータに複数のコンピュータから一斉に大量のデータを送信して負荷を掛けるなどして、そのコンピュータによるサービスの提供を不可能にするＤＤｏＳ（ディードス）攻撃やセキュリティ上のぜい弱性を悪用してコンピュータに不正に侵入する（又は不正プログラムに感染させる）ことなどにより、管理者や利用者の意図しない動作をコンピュータに命令する手法等があります。

不正プログラムに感染させる手口としては、業務に関連した正当なものであるかのように装った電子メールによる標的型メール攻撃が代表的です。



【標的型メール攻撃の例】

(2) サイバー攻撃対策の推進体制

北海道警察では、サイバー攻撃の実態解明や被害の未然防止等の総合的なサイバー攻撃対策を推進するため、北海道警察サイバー攻撃対策隊を設置しています。同隊は、サイバー攻撃捜査に関する専門的な知識、技能及び経験を生かし、情報収集活動の推進や重要インフラ事業者、民間事業者等との協力関係の確立において、中核的な役割を果たしています。

(3) 官民連携の推進

北海道警察では、サイバー攻撃による被害の未然防止や拡大防止を図るため、平素から、重要インフラ事業者等への個別訪問やサイバー攻撃対策セミナーの開催、サイバー攻撃の発生を想定した共同対処訓練の実施など、官民連携によるサイバー攻撃対策を推進しています。

また、道内の重要インフラ事業者等で構成されるサイバーテロ対策協議会を、警察本部及び全ての方面本部に設置して、サイバー攻撃の脅威や情報セキュリティに関する情報提供、民間の有識者による講演、参加事業者間の意見交換や情報共有等を行っています。