広　報　資　料

平成 24 年 8 月 23 日

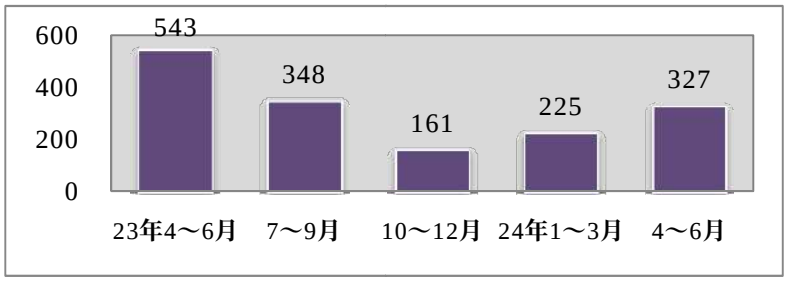
警備企画課・情報技術解析課

サイバーインテリジェンスに係る最近の情勢（平成 24 年上半期）について

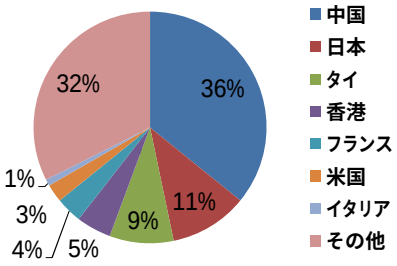
1　標的型メール攻撃事案の把握状況

○　警察では、平成 24 年上半期の間に、合計 552 件の標的型メールが我が国の民間企業等に送付されていたことを把握。

○　標的型メール攻撃に使用された不正プログラムの接続先は、約 36%が中国、約 11%が日本、約９%がタイであった。



【警察が把握した標的型メール攻撃の件数】



【不正プログラムの接続先】

2　情報窃取を企図したとみられるサイバー攻撃事案の例（詳細別紙１）

○　中国地方の事業者がのっとられ、当該企業の送付した実際のメールを利用して多数の事業者等に標的型メールが送付された事例

○　政府機関にも民間事業者等にも送付された標的型メール攻撃事例

○　多数の地方自治体等に送付された標的型メール攻撃事例

3　警察のサイバーインテリジェンス対策の取組

(1)「サイバーインテリジェンス情報共有ネットワーク」の拡充

○　警察と情報窃取の標的となるおそれのある全国の事業者等とで構築している「サイバーインテリジェンス情報共有ネットワーク」の構成員は約 4,800 の事業者等に拡大（７月１日現在）。

○　運用開始から本年６月末日までの間に、警察からの注意喚起により、各構成員は 251 件の標的型メールの送付を認知。

○　本年３月から、内閣官房と連携し、政府機関に対する標的型メール攻撃に関する情報も情報提供を始めたところ、政府機関宛てのものと同様のものが民間事業者等にも送付されていたことが判明。

(2) セキュリティ関連事業者との情報共有（詳細別紙２）

○　８月 23 日(木)、警察とセキュリティ監視サービス又はセキュリティ事案に対処するサービスを提供する事業者で構成する「サイバーインテリジェンス対策のための不正通信防止協議会」を設置。

○　情報窃取を企図したとみられるサイバー攻撃事案に係る情報共有を実施することにより、機密情報が窃取されることのないよう、事業者等が不正な接続先へ通信を行うことを防止。

別　紙　１

サイバーインテリジェンス事案の例（平成24年上半期）

１　中国地方の事業者が送付した実際のメールが利用された標的型メール攻撃事例

○　平成24年２月、中国地方のＸ社になりすました標的型メールが「サイバーインテリジェンス情報共有ネットワーク」構成員に送付されたことを把握。本ネットワーク内に注意喚起を行うとともに、Ｘ社に係る調査を実施。

○　その結果、Ｘ社の職員が取引先に対してメールを送付した約11時間後に、当該メールの本文をほとんどそのまま引用し、Ｘ社と業務上関係する２協会・４社宛てに同様の標的型メールが送付されていたことが判明。

○　また、３月には、中国地方のＹ社になりすました標的型メールが本ネットワーク構成員に送付されたことを把握。

○　Ｙ社に係る調査を実施したところ、Ｙ社の職員がＸ社の部長に対して送付したメールを窃取され、Ｘ社と業務上関係する７社宛てにこれを利用して標的型メールが送付されていたことが判明。当該標的型メールには、添付ファイルに不正プログラムが仕込まれた上、実際のメールと同様にパスワード・ロックが掛けられていた。

○　両件に使用された不正プログラムに感染したコンピュータは、いずれもタイ及び米国所在の同一のＩＰアドレスに接続する動作を行うことから、同じ攻撃者が、Ｘ社のコンピュータを乗っ取って個人情報やメールを窃取し、これを利用して、同社が業務上関係する複数の事業者等に標的型メールを送付していたものとみられる。

２　政府機関にも民間事業者等にも送付された標的型メール攻撃事例

○　４月、内閣官房情報セキュリティセンター（ＮＩＳＣ）を通じて得た標的型メール攻撃に関する情報を「サイバーインテリジェンス情報共有ネットワーク」の構成員に注意喚起したところ、同種の標的型メールが製造業者等６社にも送付されていたことが判明。

○　当該標的型メールは、職員採用に関する実在する調査の内容について記述されており、当該調査報告書を装った添付ファイル（ＰＤＦファイル）を開くと、調査報告書が表示される一方で、気付かない間にコンピュータは不正プログラムに感染する。

○　「サイバーインテリジェンス情報共有ネットワーク」内に、政府機関宛てに送付された標的型メール攻撃の情報を共有する有効性が明らかとなった。

３　多数の地方自治体等に送付された標的型メール攻撃事例

○　４月、警察庁を含む複数の省庁に対し、政府機関職員になりすまし、「対北朝鮮措置の延長について」と題した標的型メールが送付されたことを把握。「サイバーインテリジェンス情報共有ネットワーク」を通じた注意喚起を行ったところ、同様のものが２社に送付されていたことが判明。

○　さらに、複数の地方自治体から同様の標的型メールに係る情報提供を受けたことから、全国の都道府県警察に設置された「サイバーテロ対策協議会」等の枠組みを通じ、重要インフラ事業者等にも注意喚起を行ったところ、さらに23の地方自治体及び４事業者に対しても同様の標的型メールが送付されていたことを把握。

○　地方自治体が標的となった理由は不明であるが、北朝鮮の「人工衛星」と称するミサイル発射事案に乗じた標的型メール攻撃とみられる。

参　考

～地方自治体等が開設した「フォーム」等への大量送信事案～

本年６月から７月にかけて、県庁を始めとする11府県13の重要インフラ事業者等（地方自治体８、ガス２、鉄道２、空港１）が、ウェブサイトで問合せや意見等を受け付けるために開設している「フォーム」（※）と呼ばれるページに、空白や数字等の意味のない内容が、短時間に大量に送信されたり、当該事案と同じＩＰアドレスからウェブサイトに大量のアクセスが行われる事案が発生。送信元として12のＩＰアドレス（半数が中国所在のもの）が判明しており、「サイバーテロ対策協議会」等の枠組みを通じて注意喚起を実施。

※フォーム：問合せや意見等を受け付けるため、ウェブサイト管理者が選定した項目のボックスに閲覧者が情報を入力・選択できるようになっているページ。例えば、意見要望フォームでは、各項目のボックスに氏名・連絡先や意見を入力し、送信ボタンを押下することにより、情報を送信することができる。

別　紙　2

サイバーインテリジェンス対策のための不正通信防止協議会（概要）

1　設置の趣旨

サイバーインテリジェンスにより我が国から機密情報が窃取される被害を防止するため、「サイバーインテリジェンス対策のための不正通信防止協議会」を設置し、警察とセキュリティ監視サービス又はセキュリティ事案に対処するサービスを提供する事業者等との間で情報窃取を企図したとみられるサイバー攻撃事案に係る情報を共有することにより、我が国の事業者等が不正な接続先に通信を行うことの防止を図るもの。

2　運営内容

標的型メール攻撃等に利用される不正プログラムの接続先等の情報窃取を企図したとみられる不正な通信の防止に資する情報について、構成員の間で情報共有を図り、警察が直接、情報提供・注意喚起を実施している「サイバーインテリジェンス情報共有ネットワーク」を構成する事業者のみならず、セキュリティ監視サービス又はセキュリティ事案に対処するサービスを契約している我が国の事業者等に対し、これら不正な接続先への通信を防止する措置や通信を行おうとするコンピュータの特定等を推奨することなどにより、我が国の事業者等からの情報窃取を企図する不正な通信の防止のため、相互に連携を図る。

また、ＩＴユーザ全体のセキュリティの向上を図るため、本協議会を通じて得たサイバー攻撃をめぐる情勢に係る知見を活用し、必要に応じて広報を行う。

3　構成員

セキュリティ監視サービス又はセキュリティ事案に対処するサービスを提供している以下の各事業者及び警察庁とする。

- 株式会社インターネットイニシアティブ
- ＮＥＣネクサソリューションズ株式会社
- エヌ・ティ・ティ・データ先端技術株式会社
- セコムトラストシステムズ株式会社
- 日本アイ・ビー・エム株式会社
- 日本電気株式会社
- 日本電信電話株式会社
- 株式会社日立システムズ
- 三菱電機情報ネットワーク株式会社
- 株式会社ラック

サイバーインテリジェンス対策に係る警察の取組

サイバーインテリジェンス情報共有ネットワーク

サイバーフォースセンター

不正ﾌﾟﾛｸﾞﾗﾑ等の分析

ｳｲﾙｽ対策ｿﾌﾄ提供事業者

OS提供事業者

ｳｲﾙｽ対策ｿﾌﾄの更新又はOSの脆弱性解消

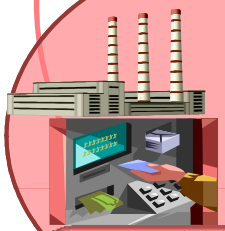
新たな不正ﾌﾟﾛｸﾞﾗﾑ・未知の脆弱性

最新の手口等

ITﾕｰｻﾞ全体のｳｲﾙｽ対策向上

サイバーインテリジェンス対策のための不正プログラム対策協議会

先端技術を有する事業者の被害防止



情報窃取の標的となるおそれのある全国約4,800の事業者等

ＣＣＩ指定事業者等

【CCI】
Counter Cyber Intelligenceの略

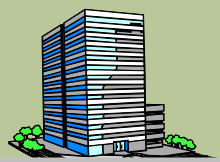
情報共有・注意喚起

標的型メールの情報提供

警察庁

情報集約・実態解明

警察



都道府県警察

不正ﾌﾟﾛｸﾞﾗﾑの接続先等の情報共有

サイバーインテリジェンス対策のための不正通信防止協議会

我が国事業者等からの不正通信の防止

ｾｷｭﾘﾃｨ監視ｻｰﾋﾞｽ提供事業者

ｾｷｭﾘﾃｨ事案に対処する事業者

我が国事業者等による不正な接続先への通信の送信防止措置の推奨等

海外の治安情報機関

情報交換