

情報技術解析平成21年報（インターネット観測結果等）について

1 概説 [4 頁]

平成21年は、米国及び韓国への大規模なサイバー攻撃、いわゆる「ガンブラー」と呼ばれる不正プログラムに関係した攻撃手法によるウェブサイト改ざんの発生、Confickerワームの感染拡大など、大きな脅威が顕在化した。これらの攻撃に見られるように、攻撃手法の巧妙化が進んでいる。

2 米国・韓国に対するサイバー攻撃 [5 頁]

平成21年7月、米国及び韓国の政府機関等35機関のウェブサイトが、3次にわたるサイバー攻撃を受けて、一時閲覧不能になった。

警察庁では、韓国の攻撃対象サイトから送信された、サイバー攻撃の影響とみられる通信を検知した。

韓国当局と連携し、我が国所在のものとして、攻撃指令を行うサーバ8台を把握した。

サイバー攻撃に利用されないため、日頃から適切なセキュリティ対策が必要である。

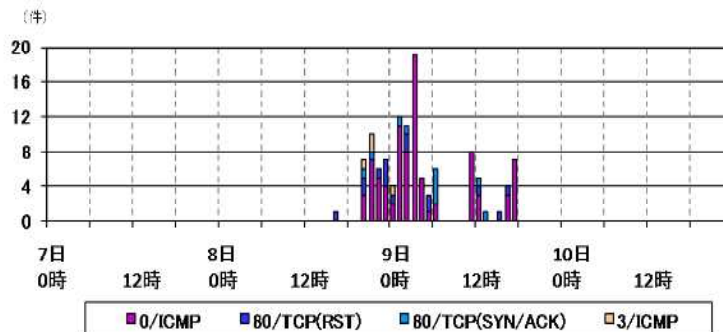


図1 韓国を発信元とするパケットの検知状況

3 「ガンブラー」によるウェブサイトの改ざん [8 頁]

平成21年中は、「ガンブラー」という攻撃手法によるウェブサイトの改ざん事案が増加した。改ざんされたウェブサイト閲覧すると、利用者が気付かないうちに特定のサイトへ誘導され、不正プログラムに感染するもの。

改ざんサイトに埋め込まれた誘導先サーバのURLをIPアドレスに変換し、そのIPアドレスを国・地域別でみると、多くがヨーロッパ所在のものであることを確認した。

被害防止のため、ウェブサイト管理用パソコンの適切な運用や管理が必要である。

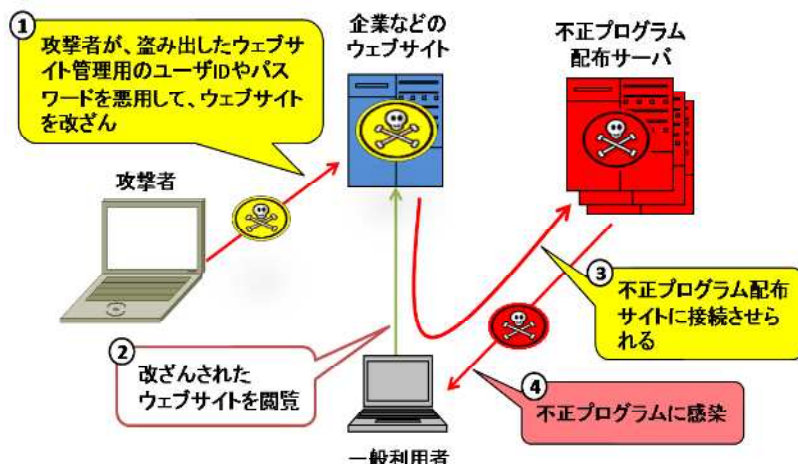


図2 不正プログラム感染までの流れ

4 Confickerワームの感染の拡大 [14頁]

平成20年以来、Windowsの特定の脆弱性を狙う「Confickerワーム」の感染拡大が継続している。警察庁でも、Confickerワームによると思われる通信の増加を確認した。

Confickerワームの駆除や新たな感染防止のため、Windowsの更新プログラムの適用やウイルス対策ソフトの適切な運用、USBメモリの自動再生機能を無効にするなどの対策が有効である。

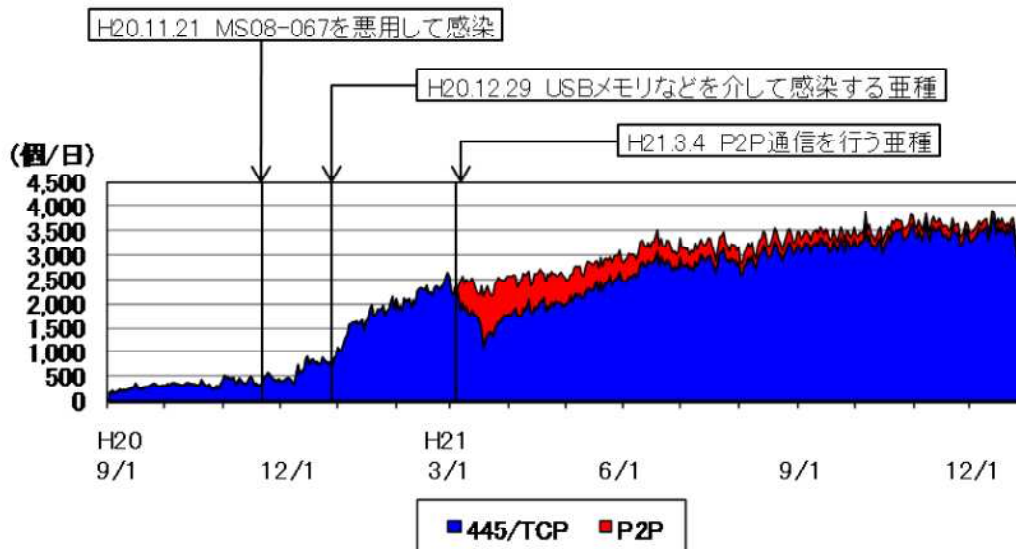


図3 Confickerの発信元IPアドレス数の推移

5 情報セキュリティの向上のために [18頁]

平成21年中のサイバー攻撃情勢を踏まえ、インターネット上の脅威から情報資産を守るために、コンピュータの利用者やサーバの管理者が採るべき基本的なセキュリティ対策を提示。

6 P2P観測システムの運用 [20頁]

平成22年1月1日からP2P観測システムの正式運用を開始した。

ファイル共有ネットワークに接続するコンピュータ数が、前年11月の一斉取締り（ファイル共有ソフトを利用した著作権法違反事件）後に約1割、本年1月の改正著作権法施行後に約2割減少した。

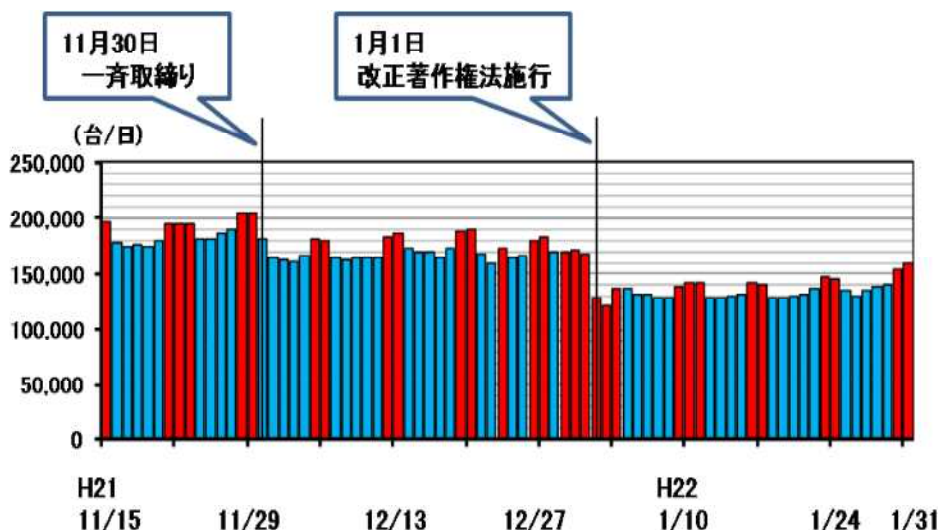


図4 接続コンピュータ数 (Share)