

「近年の標的型攻撃に関する調査研究」調査報告書の公開について

独立行政法人 情報処理推進機構（略称：IPA、理事長：藤原 武平太）は、情報システムの脆弱性対策を促進するため、特定の企業あるいは組織を標的とした攻撃を行う「標的型攻撃」に関する調査を行い、「近年の標的型攻撃に関する調査研究」として2008年3月18日（火）より、IPAのウェブサイトにて公開しました。

（URL：<http://www.ipa.go.jp/security/fy19/reports/sequential/index.html>）

近年、特定の企業あるいは組織イントラネット内のパソコンを標的とした「標的型攻撃」により、個人情報等の機密情報が漏洩するなどの被害が深刻化しています。「近年の標的型攻撃に関する調査研究」調査報告書は、こうした攻撃に利用された脆弱性の実態調査や、攻撃の際に用いられたマルウェアの分析を行い、調査報告書としてとりまとめたものです。

【従来型マルウェアとシーケンシャルマルウェア】

標的型攻撃はマルウェア（悪意あるソフトウェア）によるものが多数ですが、最近では、インターネット上の攻撃者が用意したサーバからプログラム等をダウンロードする「ダウンローダ」を介して埋め込まれる多段型のマルウェア（以下、シーケンシャルマルウェア）が多く発見されています。今回の調査の結果、シーケンシャルマルウェアの挙動を解析することで把握すると共に、「不必要な外向き TCP（Transmission Control Protocol）ポートを全て塞ぐ」等の対策が有効である事が明らかになりました（図1）。

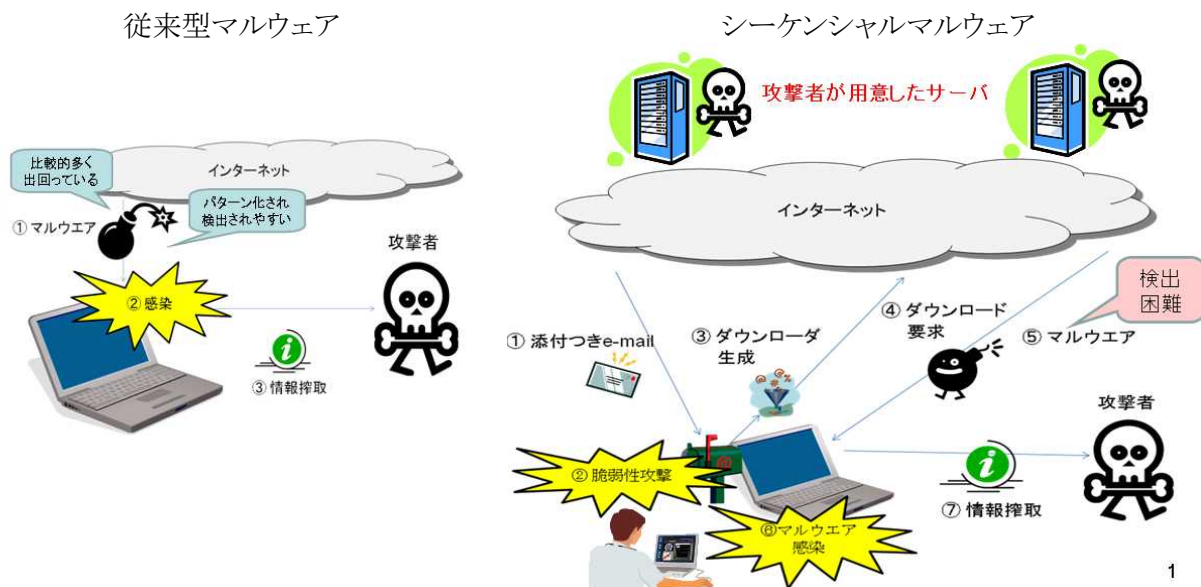


図1: 従来型マルウェアとシーケンシャルマルウェアの違い

安全な情報社会の発展のためには、標的型攻撃の脅威について広く周知を促し、対策の理解を深めることが必要です。また、有効な対策分析のためには、変化を続ける脅威に関して継続的な監視が重要です。本報告書が、標的型攻撃に対する現状分析としての有用な資料となり、セキュリティ脅威が減少することとなれば幸いです。

調査報告書の構成は以下のとおりです。

- マルウェアの解析と脅威分析
- 調査研究の範囲と調査方法
- 標的型攻撃に利用されているセキュリティ脆弱性の実態調査・傾向分析
 - ・ 標的型攻撃に利用された脆弱性
 - ・ 標的型攻撃に利用された脆弱性を持つソフトウェアやコンポーネントの傾向
- 標的型攻撃に利用されていたセキュリティ脆弱性
 - ・ 標的型攻撃に利用された脆弱性
 - ・ 標的型攻撃に利用される可能性が高いソフトウェアの傾向
- 標的型攻撃用マルウェアの実態調査・傾向分析
- 近年の標的型攻撃で用いられるマルウェアの分析
 - ・ マルウェアの解析と攻撃シーケンスの分析
 - ・ 攻撃サイトの特徴
 - ・ ボット型マルウェアと標的型攻撃マルウェアの共通仕様分析
 - ・ 標的型攻撃用マルウェアの検知手法
 - ・ 効率の良い脅威分析手法に関する検討

本書(全 36 ページ)は、次の URL よりダウンロードの上、ご参照ください。

(URL : <http://www.ipa.go.jp/security/fy19/reports/sequential/index.html>)

本件に関するお問い合わせ先

独立行政法人 情報処理推進機構 セキュリティセンター 小林／中野

Tel: 03-5978-7527 Fax: 03-5978-7518 E-mail: vuln-inq@ipa.go.jp

報道関係からのお問い合わせ先

独立行政法人 情報処理推進機構 戦略企画部広報グループ 横山

Tel: 03-5978-7503 Fax:03-5978-7510 E-mail: pr-inq@ipa.go.jp