

平成 15 年 9 月 18 日  
情報処理振興事業協会  
セキュリティセンター(IPA/ISEC)

## W32/MSBlaster 及び W32/Welchi ウイルス被害に関する企業アンケート調査の結果について

経済産業省の外郭団体である情報処理振興事業協会（略称 IPA、理事長：藤原 武平太）は、「W32/MSBlaster 及び W32/Welchi ウイルス被害に関するアンケート調査」を実施した。IPA には、8 月 12 日に MSBlaster が発見されて以来、約 10 日間で 2,000 件を超える相談・届出があったが、その殆どが個人から寄せられたものであった。そこで、今回のウイルスの被害状況をより広い観点から捉え、今後の情報セキュリティ対策に活かすために、国内企業における被害実態について緊急調査を実施したものである。

### 1. 調査目的

インターネットが企業、学校、家庭に普及している現在では、コンピュータウイルス（以下、ウイルス）の急速な感染の拡大によって大規模な障害が発生した場合、その社会的影響は計り知れない。このためウイルス対策やセキュリティ上の脆弱性についての対策が、重要な課題となっている。

今回のマイクロソフト社の Windows XP 等に存在するセキュリティ上の脆弱性を攻略して感染を拡大するワームである W32/MSBlaster（以下、「MSBlaster」）及び W32/Welchi（以下、「Welchi」）については、急激な感染の拡大と、多大な被害が報告されている。

IPA においては、8 月 12 日に MSBlaster が発見されて以来、約 10 日間で累計 2,000 件以上の相談・届出が寄せられたが、その殆どが個人からのものであった。そこで、今回のウイルスの被害状況をより広い観点から把握し、情報セキュリティ対策の基礎資料とするとともに、今後起こり得る同様なインシデントへの対する対策の策定に資するため、緊急の国内企業アンケート調査を実施した。

### 2. 調査方法

調査期間： 2003 年 8 月 28 日 ~ 2003 年 9 月 11 日

調査方法： 電話調査（一部ファクシミリを併用）

調査対象： 国内民間企業本社（\*1）

\*1 主にシステム管理部門担当者に相当する職員に回答を求めた。

有効回答数： 985 社（\*2）

\*2 以下では設問に対する有効回答数を n と表記する。

### 3. 被害実態

MSBlaster 及び Welch は、OS としては主に Windows XP や Windows 2000 を感染対象とするウイルスである。これらの導入状況に関する設問への回答があった 982 社のうち、88.4% の企業が、これらの OS が搭載された PC を所有しており、台数ベースでは全体で約 180,000 台のうち 41.1% にこれらの OS が搭載されていた。

ウイルスの影響を受ける可能性があるこれらの PC を持つ企業のうち、18.6% の企業が MSBlaster あるいは Welch に感染していた。特に従業員数 100 名以上の企業においては、感染があった企業は 23.4% と高い割合であった。

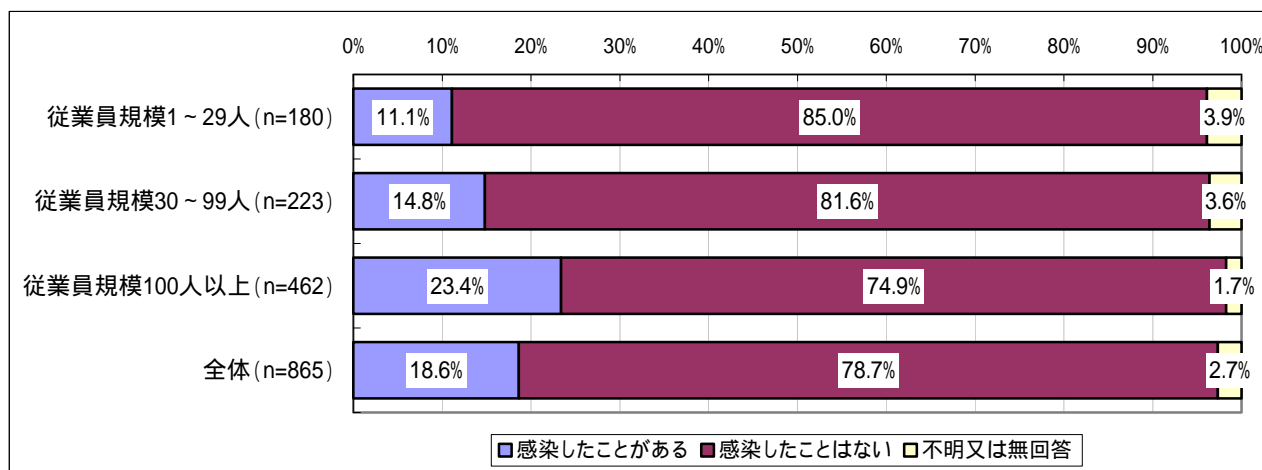


図1 MSBlaster、Welchi への感染の有無

MSBlaster もしくは Welch に感染した日については、共に 8 月 18 日が最も多かった。

8 月 18 日はお盆休み明けの月曜日であり、始業と共に感染が広がったと思われる。休暇中に自宅に持ち帰った PC を会社のネットワークに接続して感染したケースも多かったと考えられる。また、8 月 18 日は Welch が新種として確認された日でもあった。

(n=164)

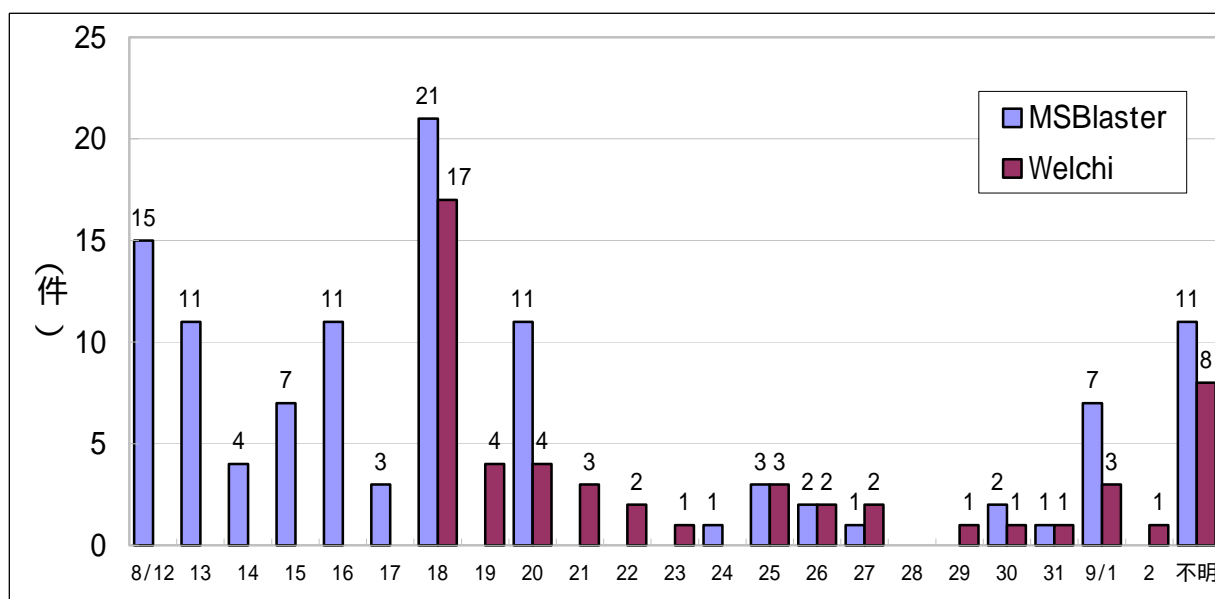


図2 MSBlaster、Welchi への感染日

MSBlaster および WelchI については、脆弱性を持つ PC をインターネットに接続しただけで感染する可能性がある。

システム管理者が想定する感染経路については、25.0%が「持ち込んだパソコンから」の感染を想定していた。

(n=160)

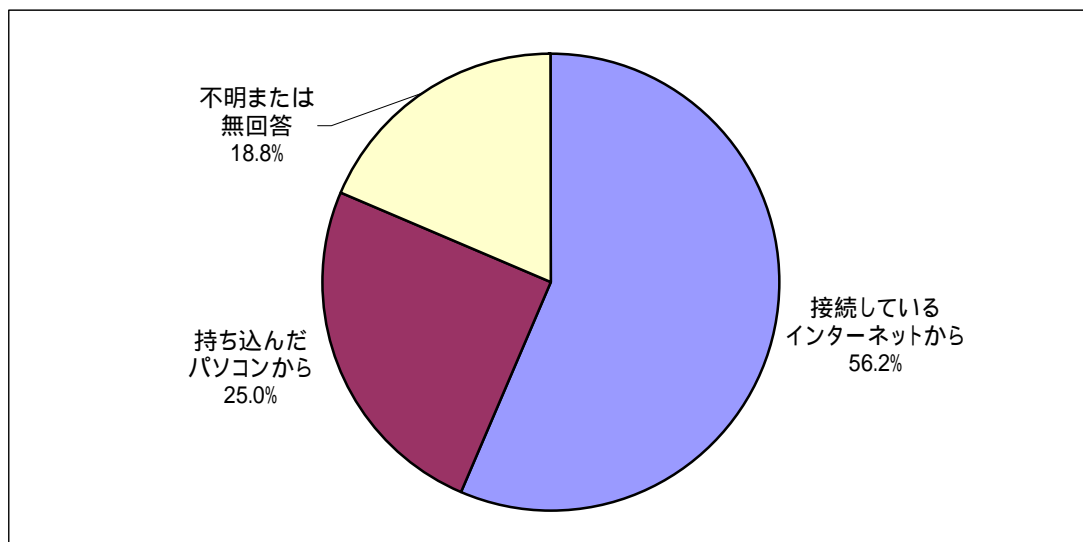


図3 想定される感染経路

ウイルスの発見から復旧にまでに要した時間については、「およそ1日程度」とした企業が26.1%と最も多かった。感染被害があった企業の50%以上が復旧に1日以上を必要とした。復旧までに10日以上かかった企業も3.2%ほどあり、被害の長期化が見られた。

(n=157)

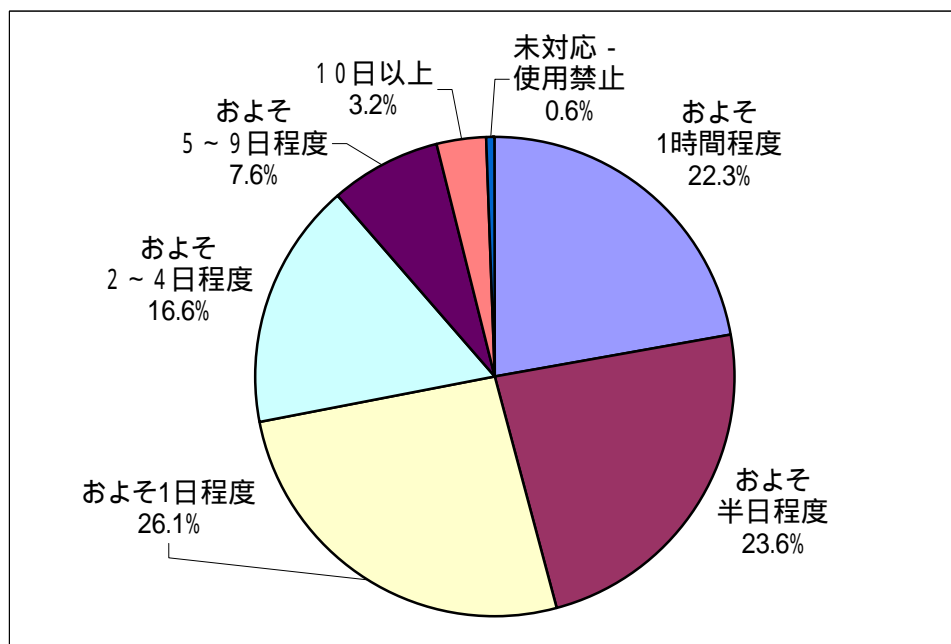
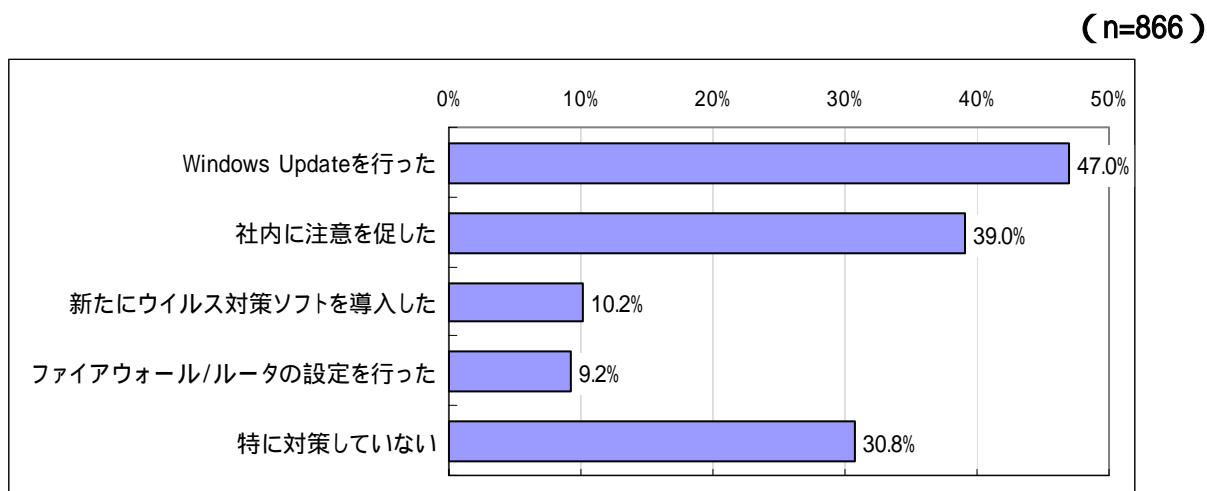


図4 発見から復旧までに要した時間

## 4. 対策の状況

MSBlaster、Welchi への対策のためには、マイクロソフト社が提供する修正プログラム適用サービスである Windows Update 等の手段により、脆弱性を修正することが不可欠である。

これらのウイルスに関して特別に取った対策について尋ねたところ、Windows Update により脆弱性対策を行った企業は 47.0%と約半数であり、十分に対策が取られたとは言い難い状況であった。



(複数回答)

図5 MSBlaster、Welchi への対策

普段の Windows Update の実施については、全体の 47.9%が「各ユーザ任せ」であった。これは、従業員数が多い企業ほど高くなる傾向がみられ、セキュリティ対策の状況把握と徹底が不十分な現状が伺われた。

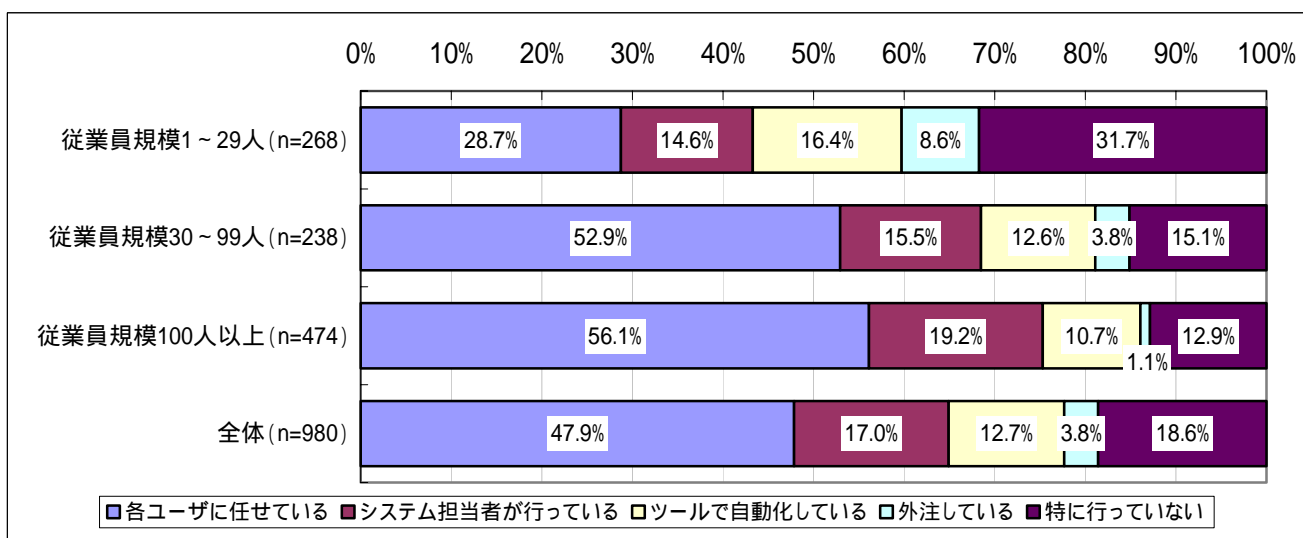
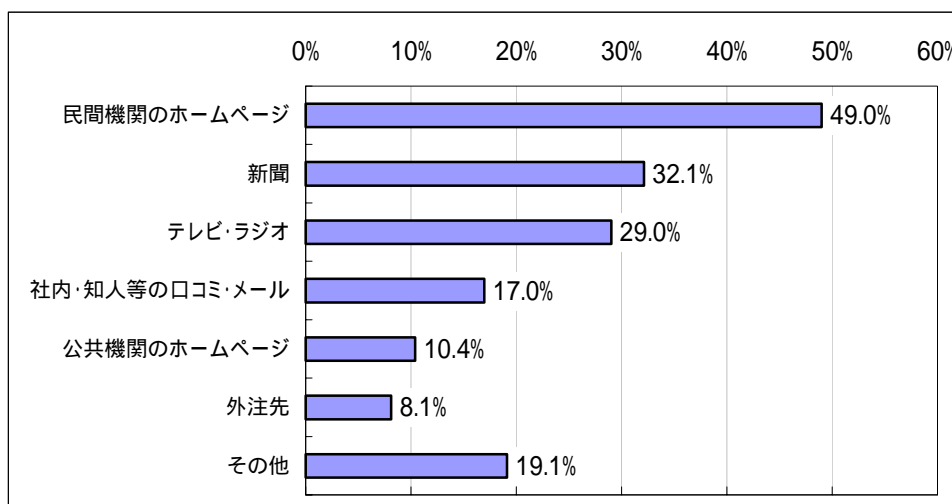


図6 Windows Update の実施方法

対策のきっかけとなった情報源については、調査対象の企業からは「民間機関のホームページ」が49.0%と最も多く挙げられた。「新聞」「テレビ・ラジオ」を情報源として挙げた企業もそれぞれ30%前後と多く、今回のマスメディアによる報道には、個人ユーザへの対策を促すだけでなく、企業の対策を促す上でも効果があったと言える。

(n=837)



(複数回答)

図7 MSBlaster、Welchi の対策のきっかけとなった情報源

## 5. 分析

多数の従業員を抱える企業においては、セキュリティ対策の対象となるPCの台数が増えるに従い、ひとりのシステム管理者が管理を担当する台数が増え、対策の徹底がより難しくなっていると推測される。これは、従業員規模100名以上の企業においては、脆弱性修正についてユーザ任せにする率が高く、MSBlasterおよびWelchiの感染率も高くなっていることから裏付けられる。

今後は、特に大企業においては、システム管理者の作業負担を軽減し、脆弱性対策の徹底を促すためのツール等の利用が不可欠だろう。

本調査に関する詳細な報告は、IPAのWebサイトにおいて9月下旬を目処に公開予定である。

問合せ先：情報処理振興事業協会 セキュリティセンター（IPA/ISEC）石井、笠井、井上  
 （ISEC: Information technology SEcurity Center）  
 TEL:03-5978-7508 FAX:03-5978-7518 E-mail:isec-info@ipa.go.jp  
<http://www.ipa.go.jp/security/>