IPA テクニカルウォッチ

企業における情報セキュリティ対策効果に関する検証
～ウイルス感染リスクを低減する効果的な対策が明らかに～

2014年3月19日

独立行政法人情報処理推進機構
技術本部 セキュリティセンター
目次

1. はじめに ................................................................................................................................. 2
2. 調査データ（アンケート調査の概要と分析手法） ................................................................. 2
  2.1. 調査対象企業 .................................................................................................................. 2
  2.2. ウイルス対策項目の抽出 ............................................................................................... 3
  2.3. 対策状況とウイルス感染率の関係、及び分析手法 ............................................................... 4
3. 分析結果 ................................................................................................................................ 6
  3.1. 基本ケースの分析 .............................................................................................................. 6
  3.2. 基本ケースの拡張分析 ..................................................................................................... 7
    3.2.1. 中小企業/大企業のケース ........................................................................................ 8
    3.2.2. 非製造業/製造業のケース ......................................................................................... 8
    3.2.3. WCF 及び R_in/out いずれも未導入/少なくともどちらかは導入のケース ........... 9
  3.3. セキュリティ対策推進への適用 ...................................................................................... 10
4. おわりに .................................................................................................................................. 10
1. はじめに

近年、不正アクセスによるウェブ改ざん、改ざんされたウェブサイトからのウイルス感染、標的型攻撃による情報漏えいなど、いわゆる情報セキュリティインシデントが多発し、その結果、情報セキュリティの重要性が多くの組織に認識されることとなった。2012年にIPAが行った企業を対象とした調査によると、回答企業のほぼ全てが、情報セキュリティ確保のため、何らかの対策を講じていると回答している。しかし、多くの対策のうち、どの対策がどの程度セキュリティ確保に寄与しているのかに関して、科学的な分析による効果は、殆ど知られていないのが現状である。

本レポートでは、どのような情報セキュリティ対策（以下、対策）が、組織のセキュリティインシデントに遭遇する危険を低減させる効果を持つのかについて、企業を対象としたアンケート調査のデータを元に検証する。情報セキュリティインシデントの中でも、被害の報告件数が最多で、それ故今後も多くの組織が遭遇する可能性があるウイルス感染に焦点を当てる。そして、どのような対策がウイルス感染リスクを低減する効果があるのかを統計を利用して分析する。

本レポートの構成は、次の第2章で分析に用いたデータの概要と分析手法について、第3章で分析結果を提示し、第4章で結果のまとめとなっている。

2. 調査データの概要と分析手法

本レポートでは、「2011年度情報セキュリティ事象被害状況調査」（以下、IPA調査）のデータを用いて分析している。同調査では企業に対し、主に（1）2011年4月〜2012年3月の間（以下、2011年度）にどのような対策が講じられていたか（2）2011年度に何らかの情報セキュリティインシデントに遭遇したか（3）遭遇した場合の被害状況（4）基本情報（従業員数、業種、売上高等々）の事柄に関して尋ねている。

2.1. 調査対象企業

回答企業は1,767社であり、そのうち業種に関して未回答の企業を除く1,727社の業種別（製造業、非製造業）、企業規模別の内訳は、表1の通りである。（本レポートでは、従業員数300人未満の企業を「中小企業」、300人以上を「大企業」とする）。

分析対象は、全回答企業1,767社ではなく、2011年度にコンピュータウイルスに遭遇したと回答した1,130社（表2-1の赤字部）とする。何故なら、これらの企業のみが、分析に必要な情報（導入されている対策が実際にウイルス感染を防いだか否か）を提供しているからである。これらの企業に関して、業種別、規模別に分けたものを表2-2、2-3にそれぞれ示す。

1 本レポートは経済産業研究所のホームページにて発表されたIPAと経済産業研究所の共同研究論文（以下、DP）http://www.rieti.go.jp/jp/publications/summary/13100004.htmlを基に再構成したものである。
2 IPA調査に回答していただいた組織、団体の中には企業だけでなく、非営利団体も少なからずあるが、本レポートでは全ての団体を一括して企業と呼ぶこととする。
2.2. ウイルス対策項目の抽出

対策の効果を測定するため、ウイルス遭遇経験のある1,130社がウイルス遭遇時に以下の9つの対策を講じていたかに関するデータを利用して、これら9つの対策は、IPA調査で導入の有無を尋ねた全対策のうち、製造業のウイルス感染防止に貢献すると考えられるものであり、直接的に影響のありそうな対策（技術的対策）、間接的に影響のありそうな対策（運用的対策、人的対策（教育））を抽出した。

1. セキュリティソフト（ネットワークサーバー用）
2. セキュリティソフト（クライアントPC用）
3. プロバイダによるウイルスチェック
4. ウェブ閲覧フィルタ（以下、WCF）
5. 検疫ネットワーク
6. 機器や記録媒体の持ち込み・持出しの制限（以下、R_in/out）
7. セキュリティパッチ適用
8. 情報セキュリティ教育
9. セキュリティ監査

これら9つの対策が対象企業において、どの程度の割合で導入されていたのかを表3に示す。業種、規模に関わらず、セキュリティソフトは非常に多くの企業で導入されている。更に、R_in/out、セキュリティパッチなども半数以上の企業で導入されている。反対に、情報セキュリティ監査、そして特に検疫ネットワークはそれほど利用されていないことがわかる。企業規模別にみると、大企
業の方が中小企業より多くの対策で導入率が高く、業種別で見ると製造業の方が非製造業より多くの対策で導入率が高いことも分る。

<table>
<thead>
<tr>
<th>表 3：対策導入率</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>全体 (N=742)</th>
<th>企業規模 (N = 742)</th>
<th>業種 (N = 723)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>中小企業 (N=267)</td>
<td>大企業 (N=475)</td>
</tr>
<tr>
<td>---------------</td>
<td>-----------------</td>
<td>----------------</td>
</tr>
<tr>
<td>セキュリティソフトネットワークサーバ用</td>
<td>90.97%</td>
<td>85.39%</td>
</tr>
<tr>
<td>セキュリティソフトウェア</td>
<td>97.71%</td>
<td>96.25%</td>
</tr>
<tr>
<td>クライアントPC用プロバイダによるウイルスチェック</td>
<td>50.40%</td>
<td>53.56%</td>
</tr>
<tr>
<td>WCF</td>
<td>59.30%</td>
<td>40.82%</td>
</tr>
<tr>
<td>検疫ネットワーク</td>
<td>14.82%</td>
<td>10.11%</td>
</tr>
<tr>
<td>R_in/out</td>
<td>75.88%</td>
<td>63.67%</td>
</tr>
<tr>
<td>セキュリティパッチ</td>
<td>75.34%</td>
<td>61.42%</td>
</tr>
<tr>
<td>情報セキュリティ教育</td>
<td>61.19%</td>
<td>43.82%</td>
</tr>
<tr>
<td>セキュリティ監査</td>
<td>42.32%</td>
<td>32.96%</td>
</tr>
</tbody>
</table>

2.3. 対策状況とウイルス感染率の関係、及び分析手法

表 2-2、2-3、及び 3 の集計結果を統合することにより、個々の対策の導入・未導入とウイルス感染率との関係について知ることが出来る。表 4 にその関係を示す。これによると、対策を導入しているグループの方が未導入のグループより感染率が明らかに低いと言う直感的に納得のいくケースが多数存在するものの、これとは逆に導入グループの方が感染率が高いケースも少なくなず存在していることが分かる。（例えば、「全体」の列の「セキュリティソフトネットワークサーバ用」の結果を見ると、導入グループの感染率が 26.22% な対し、未導入グループの感染率は 23.88% である。）

---

3 表 3 で、対象企業数が 1,130 社から大幅に減っているが、これは各対策の導入に関する質問に無回答であった企業を除外したためである。
この集計結果から、たとえば、「WCF」と「R_in/out」については、企業規模、業種に関わらず導入グループの方が未導入グループより感染率が低いので、ウイルス感染リスクの低減効果があると言えるのであろうか？ 或いは、「セキュリティソフトクライアント PC用」については、中小企業、非製造業ではそのような効果があると言うのは妥当であろうか？ 表4の結果だけでは、そのように判断することはできない。ある対策について、ウイルス感染リスクの低減効果があると判断するには、単なるクロス集計の結果ではなく何らかの判断材料が必要となってくる。

ここでは、そのような判断材料を得るために、経済学において二者択一的な状況を実証的に分析する際に使われるプロビット回帰分析4を行う。プロビット回帰分析では、個人がある行動をとるか否かの状況で、その行動をとる確率を数式で表し、その確率を上げるもしくは下げる要因が何かを統計学的手法を用いて検証する。ここでは、企業がウイルスに感染するか否かの状況で、「感染する」確率を数式で表し、どの対策に統計学的に有意なウイルス感染確率の低減効果があるのか分析する。その結果を基に個々の対策の感染リスク低減効果の有無を判断する。

※括弧内の数値は企業数を表している。

<table>
<thead>
<tr>
<th></th>
<th>全体 (N = 742)</th>
<th>企業規模 (N = 742)</th>
<th>業種 (N = 723)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>導入</td>
<td>未導入</td>
<td>導入</td>
</tr>
<tr>
<td>セキュリティソフトネットワークサーバ用</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>導入</td>
<td>26.22% (177)</td>
<td>21.05% (48)</td>
<td>28.86% (129)</td>
</tr>
<tr>
<td>未導入</td>
<td>23.88% (16)</td>
<td>20.51% (8)</td>
<td>28.57% (6)</td>
</tr>
<tr>
<td>セキュリティソフトクライアントPC用</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>導入</td>
<td>25.93% (188)</td>
<td>20.23% (52)</td>
<td>29.06% (136)</td>
</tr>
<tr>
<td>未導入</td>
<td>29.41% (5)</td>
<td>40% (4)</td>
<td>14.29% (1)</td>
</tr>
<tr>
<td>プロバイダによるウイルスチェック</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>導入</td>
<td>24.87% (93)</td>
<td>17.48% (25)</td>
<td>29.44% (68)</td>
</tr>
<tr>
<td>未導入</td>
<td>27.17% (100)</td>
<td>25% (31)</td>
<td>28.28% (69)</td>
</tr>
<tr>
<td>WCF</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>導入</td>
<td>23.18% (102)</td>
<td>15.60% (17)</td>
<td>25.68% (85)</td>
</tr>
<tr>
<td>未導入</td>
<td>30.13% (91)</td>
<td>24.68% (39)</td>
<td>36.11% (52)</td>
</tr>
<tr>
<td>検疫ネットワーク</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>導入</td>
<td>25.45% (28)</td>
<td>18.52% (5)</td>
<td>27.71% (23)</td>
</tr>
<tr>
<td>未導入</td>
<td>26.11% (165)</td>
<td>21.25% (51)</td>
<td>29.08% (114)</td>
</tr>
<tr>
<td>R_in/out</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>導入</td>
<td>24.16% (136)</td>
<td>18.82% (32)</td>
<td>26.46% (104)</td>
</tr>
<tr>
<td>未導入</td>
<td>31.84% (57)</td>
<td>24.74% (24)</td>
<td>40.24% (33)</td>
</tr>
<tr>
<td>セキュリティパッチ</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>導入</td>
<td>27.55% (154)</td>
<td>20.12% (33)</td>
<td>30.63% (121)</td>
</tr>
<tr>
<td>未導入</td>
<td>21.31% (39)</td>
<td>22.33% (23)</td>
<td>20% (16)</td>
</tr>
<tr>
<td>情報セキュリティ教育</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>導入</td>
<td>25.55% (116)</td>
<td>18.80% (22)</td>
<td>27.89% (94)</td>
</tr>
<tr>
<td>未導入</td>
<td>26.74% (77)</td>
<td>22.67% (34)</td>
<td>31.16% (43)</td>
</tr>
<tr>
<td>セキュリティ監査</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>導入</td>
<td>25.93% (111)</td>
<td>24.02% (43)</td>
<td>27.31% (68)</td>
</tr>
<tr>
<td>未導入</td>
<td>26.11% (82)</td>
<td>14.77% (13)</td>
<td>30.53% (69)</td>
</tr>
</tbody>
</table>

4 プロビット回帰分析とは、例えば、個人が車を購入するか否か、主婦がパートで働くか否かの決定要因を分析する際等に使われる。詳細については、DPを参照されたい。なお、回帰分析においては、対策だけでなく、各企業の属性に関する情報（従業員数、企業でのIT使用の程度、上場有無、海外展開の有無、特定業種（金融・保険、教育業）に属しているかどうか）なども併せて使用している。
分析にあたっては、図1に示すように、対策に関する情報のみを使ったモデル1、対策に加えて脚注4にある企業属性を表す情報全てを使ったモデル5など5つのモデルを考え、それぞれのモデルにおいてプロビット回帰分析を行った。

3. 分析結果

3.1. 基本ケースの分析

まず、前述した5つのモデルそれぞれでプロビット回帰分析を行い、その結果を表5にまとめた。「WCF」と「R_in/out」は全てのモデルの結果が統計学的に有意な感染リスク低減効果があることを示唆していた。

これらの対策に効果がある理由は、主要なウイルス感染経路向けの対策であるということに関係していると考えられる。IPA調査によると、ウイルス遭遇企業のうち、62％がWebページ経由で、46％の企業がUSBメモリなどの外部記憶媒体経由でウイルスが侵入したと考えている。そのような経路への対策だからこそ効果があるという点は納得のいく結果と言える。

対策のみを含んだモデル1だけではなく、企業属性も含んだモデル2～5を採用した理由は統計学上の理由による。興味のある方はDPを参照されたい。

「WCF」と「R_in/out」以外の対策に関して、どのモデルからも統計学的に有意な感染リスク低減効果があることを示唆する結果は得られなかったが、その対策自体にそもそも感染リスク低減効果が無いと言っているわけではない点に注意されたい。
それでは、これらの対策がどの程度感染確率を低減させるのであろうか？企業の実際の感染確率を知ることは出来ないので、それについては不明である。しかし、代替案としてプロピット回帰分析の結果から、各企業が「WCF（或いは R_in/out）」を導入している場合の感染確率、未導入の場合の感染確率を推計し、下式のように、両者の差から効果の度合いに関して計算することは可能である。

\[
\frac{1}{n-1} \sum_{i=1}^{n} \left( \left( \text{企業} \ i \ 	ext{が WCF（或いは R_in/out）を導入している場合の推計感染確率} \right) - \left( \text{企業} \ i \ 	ext{が WCF（或いは R_in/out）を導入していない場合の推計感染確率} \right) \right)
\]

その計算を行った結果、「WCF」、「R_in/out」どちらの対策も推計感染確率を平均的に 10%前後低減させる効果があることが判明した。

### 3.2. 基本ケースの拡張分析

「3.1 基本ケースの分析」では、どの対策がウイルス感染の低減効果が期待できるのか検証した。これを拡張し、「あるグループでは、統計学的に有意なウイルス感染リスク低減効果があるが、（対になる）別のグループでは統計学的に有意な低減効果が期待できない対策はあるのか？ある場合、どのグループのどの対策なのか？」を検証する。ここで取り上げるのは以下の 3つのケースである。

1. 中小企業／大企業
2. 非製造業企業／製造業企業
3. WCF、及び R_in/out のいずれも未導入の企業のグループ／少なくともどちらか一方は導入している企業のグループ

<table>
<thead>
<tr>
<th>モデル</th>
<th>対策</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
</tr>
</thead>
<tbody>
<tr>
<td>セキュリティソフトネットワークサーバ用</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>セキュリティソフト</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>クライアントPC用</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>プロバイダによるウイルスチェック</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>WCF</td>
<td>○</td>
<td>○</td>
<td>○</td>
<td>○</td>
<td>○</td>
<td></td>
</tr>
<tr>
<td>検疫ネットワーク</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>R_in/out</td>
<td>○</td>
<td>○</td>
<td>○</td>
<td>○</td>
<td>○</td>
<td></td>
</tr>
<tr>
<td>セキュリティパッチ</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>セキュリティ教育</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>セキュリティ監査</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

表内の○は、その対策が統計学的に見て有意なウイルス感染リスク低減効果があることを示している。空白はそのような効果があるという結果がプロピット分析から得られなかったことを意味する。
3.2.1. 中小企業／大企業のケース
データセットを中小企業のデータ、大企業のデータに分割し、それぞれのデータを用いて、ブロビット回帰分析を行った。結果は表6の通りである。

表6：ウイルス感染リスク低減効果のある対策（企業規模別）

<table>
<thead>
<tr>
<th></th>
<th>中小企業</th>
<th>大企業</th>
</tr>
</thead>
<tbody>
<tr>
<td>プロバイダによる</td>
<td>セキュリティソフト</td>
<td>セキュリティソフト</td>
</tr>
<tr>
<td>メールモデル1</td>
<td>モデル2</td>
<td>モデル3</td>
</tr>
<tr>
<td>R_in/out</td>
<td>セキュリティパッチ</td>
<td>情報セキュリティ</td>
</tr>
<tr>
<td>モデル1</td>
<td>モデル2</td>
<td>モデル3</td>
</tr>
<tr>
<td>プロバイダによる</td>
<td>セキュリティソフト</td>
<td>セキュリティソフト</td>
</tr>
<tr>
<td>メールモデル1</td>
<td>モデル2</td>
<td>モデル3</td>
</tr>
<tr>
<td>R_in/out</td>
<td>セキュリティパッチ</td>
<td>情報セキュリティ</td>
</tr>
<tr>
<td>モデル1</td>
<td>モデル2</td>
<td>モデル3</td>
</tr>
</tbody>
</table>

※表6中の「〇」、及び空白の解釈は表5と同じ

「WCF」、「R_in/out」は大企業では感染リスクの低減効果があるという結果が出たが、中小企業ではそのような結果は出なかった。「セキュリティソフトクライアント PC用」に関しては、大企業では感染リスクの低減効果があるという結果がどのモデルからも得られず、中小企業でもモデル2でしか、そのような結果が得られなかった。それ故、中小企業では統計学的に有意な低減効果があるが大企業ではそのような効果が期待できるとは言えないと結論づけるには根拠が不十分である。

3.2.2. 非製造業／製造業のケース
データセットを非製造業企業のデータ、製造業企業のデータに分割し、前節と同様の分析を行った。結果は表7の通りである。「R_in/out」、「情報セキュリティ教育」は、非製造業企業では統計学的に有意な感染リスク低減効果があるが、製造業企業ではそのような効果があることを示す結果が得られなかった。「WCF」については、非製造業企業ではリスク低減効果が期待できるが、製造業企業ではモデルによって異なる結果が得られたので、そのような効果が期待できると考えるには根拠が不十分である。

---

※この研究では、モデル1、2、5の結果のみを提示する。これ3つのモデルで同じ結果が出た場合（ある対策に関して、統計学的に有意なウイルス感染確率低減効果があるという結果が得られた）が結果を得られなかった。モデル3、4でも同じ結果が得られたことは確認済みである。
3.2.3. WCF 及び R_in/out いずれも未導入/少なくともどちらかは導入のケース

これまで多くのケースで、「WCF」、「R_in/out」に統計学的に有意なウイルス感染確率の低減効果があるという結果が得られた。この結果の通り両対策が本当に有効であれば、少なくとも「WCF」、「R_in/out」のどちらか一つが企業に導入されていれば、その企業のウイルス感染リスクが既に低い状態にあるはずである。そのような状況であれば、「WCF」、「R_in/out」以外のどの対策を導入しても、統計学的に有意な感染リスクの低減効果をもたらすのではなないだろうか？逆に言えば、「WCF」、「R_in/out」のいずれも導入されていない時のみ、それらの対策（WCF、R_in/out 以外の対策）のいずれかがリスク低減効果をもたらし得るのではないだろうか？

この仮説を検証するために、「WCF」、「R_in/out」のいずれも未導入の企業グループ、少なくともどちらか一方は導入しているグループにデータを分割し、両グループについてプロビット回帰分析を行った。その結果を表 8 に示す。

「セキュリティソフトクライアント PC 用」についてのみ、（仮説通りに）「WCF」、「R_in/out」のいずれも導入されていない場合に、統計学的に有意なウイルス感染リスクの低減効果があることが分かった。この結果は、「WCF」、「R_in/out」のどちらか一方でも導入されれば、ウイルス感染防止対策としてのソフトウェアはそれらに取って代わられるということ、つまり「セキュリティソフト」と「WCF」や「R_in/out」との間に代替効果があることを示唆している。

<table>
<thead>
<tr>
<th>表 8：ウイルス感染リスク低減効果のある対策（WCF、R_in/out の導入有無別）</th>
</tr>
</thead>
<tbody>
<tr>
<td>WCF &amp; R_in/out 未導入</td>
</tr>
<tr>
<td>セキュリティソフトネットワークサーバ用</td>
</tr>
<tr>
<td>モデル1</td>
</tr>
<tr>
<td>○</td>
</tr>
<tr>
<td>セキュリティバックアップ</td>
</tr>
<tr>
<td>モデル1</td>
</tr>
<tr>
<td>WCF &amp; R_in/out 基準</td>
</tr>
<tr>
<td>セキュリティソフトネットワークサーバ用</td>
</tr>
<tr>
<td>モデル1</td>
</tr>
<tr>
<td>追加</td>
</tr>
<tr>
<td>R_in/out</td>
</tr>
<tr>
<td>情報セキュリティ教育</td>
</tr>
<tr>
<td>モデル1</td>
</tr>
</tbody>
</table>

※表 8 中の「〇」、及び空白の解釈は表 5 と同じ
3.3. セキュリティ対策推進への適用

これまでの分析結果の含意として、次のようなことが言える。情報セキュリティ対策レベルの向上のため、ウイルス感染防止に関しては、今後は「WCF」並びに「R_in/out」（更に業種によっては情報セキュリティ教育）の導入に力点を置いた対策が適切であることが示唆された。対策効果の期待できる大企業や非製造業には、とりわけ強く提唱していくべき対策項目である。

一方、情報セキュリティ対策予算の不足、或いは情報セキュリティ要員の不在等などの理由から「WCF」、「R_in/out」の導入が難しい企業に対しては、少なくとも「セキュリティソフト（クライアント PC用）」の導入及び定期的なアップデートを行うよう提唱していくべきである。

4. おわりに

本レポートは、どの情報セキュリティ対策にコンピュータウイルス感染リスク低減効果があると考えられるのか、プロビット回帰分析を用いて検証を行った。

その結果、「WCF」、「R_in/out」の2つの対策は統計学的に有意な感染確率の低減効果をもたらすことが分かった。更に、どちらかの対策を導入した場合、どの程度感染リスクを低減させると考えられるか推計してみたところ、いずれの対策も推計感染確率を平均的に10%前後減少させるという結果が得られた。

対策の効果について、企業規模別、業種毎に更なる分析を行った結果、上記2つの対策は、大企業では感染リスク低減効果が期待できるが、中小企業では統計学的に見て有意な低減効果をもたらすという結果は得られなかった。非製造業/製造業の分析では、「R_in/out」と「情報セキュリティ教育」については、非製造業でのみ統計学的に有意な効果があることが分かった。「WCF」及び「R_in/out」未導入の企業のグループと少なくともどちらか一方は導入している企業のグループを比べたところ、「セキュリティソフト（クライアント PC用）」については、前者においてのみ統計学的に有意な感染リスクの低減効果が期待できることが分かった。
IPA テクニカルウォッチ

企業における情報セキュリティ対策効果に関する検証

～ ウイルス感染リスクを低減する効果的な対策が明らかに ～

[発行] 2014年3月19日
[著作・制作] 独立行政法人情報処理推進機構 技術本部 セキュリティセンター
[執筆者] 飯高雄希 小松文子