

「JPCERT/CC レポート読者アンケート調査および分析」  
調査結果報告書  
(2005年9月アンケート実施)

有限責任中間法人JPCERTコーディネーションセンター

## 目次

1. 調査の枠組み
2. 調査結果
  - 2.1 JPCERT/CC レポートの利用状況
  - 2.2 JPCERT/CC レポートに対する評価、要望
  - 2.3 JPCERT/CC以外の、脆弱性情報、インシデント情報の主な入手先
  - 2.4 JPCERT/CC レポートの利用期間
  - 2.5 PGP署名について
  - 2.6 回答者のプロフィール

## 1. 調査の枠組み

### ◆ 調査目的

発行開始以来4年が経過するJPCERT/CCレポートの読者に対し、JPCERT/CCレポートの利用方法や内容に関する期待・要望をアンケートによって調査し、今後のJPCERT/CCレポートの内容の改善を図る。

### ◆ 調査対象

JPCERT/CCレポートを配布するメーリングリスト(announce ML)の登録者、ならびにWeb上のJPCERT/CCレポート読者。

### ◆ 調査手法

- ・Webによるアンケート
- JPCERT/CCレポート中でアンケート実施を告知
- JPCERT/CC Webサイトのトップページでアンケート実施を告知
- ・回答者は指定のURLにアクセスし、提示されたアンケートに回答

### ◆ 調査期間

2005年9月7日(水)～22日(木)(16日間)

### ◆ 回答件数

有効回答 355件

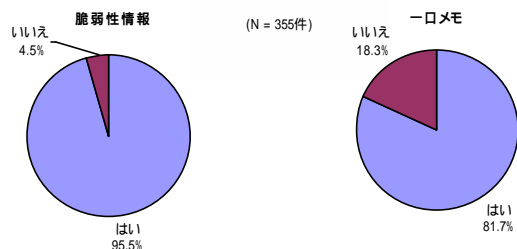
## 2. 調査結果

### 2.1 JPCERT/CC レポートの利用状況

#### JPCERT/CC レポートの利用の有無

脆弱性情報を利用している」との回答は全回答件数(355件)の95.5%、「一口メモを利用している」との回答は81.7%であった。また、80.8%が脆弱性情報と一口メモの両方を利用していると回答した。

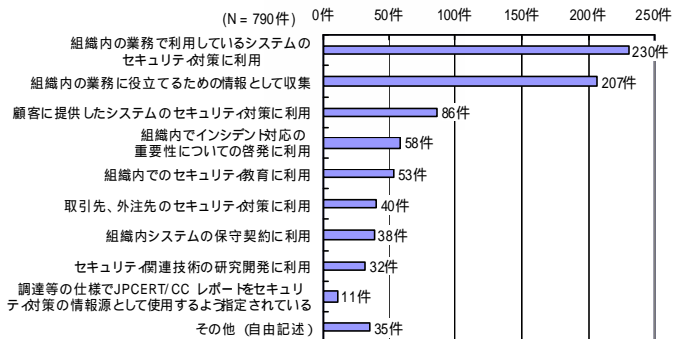
#### JPCERT/CC レポートの利用の有無



### JPCERT/CC レポートの利用方法

JPCERT/CC レポートの利用方法の上位2つは「組織内の業務で利用しているシステムのセキュリティ対策」、「組織内の業務に役立てるための情報の収集」であり、ともに全回答件数(355件)の約6割と突出している。また、第3位の「顧客に提供したシステムのセキュリティ対策に利用」を含め、主にセキュリティ対策等の業務に利用されていることがわかる。

JPCERT/CC レポートの利用方法 (複数回答)



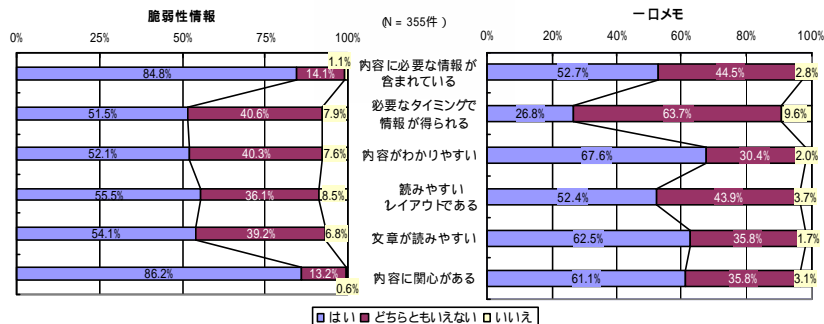
## 2.2 JPCERT/CC レポートに対する評価、要望

### JPCERT/CC レポートの内容に対する評価

脆弱性情報については、全回答件数(355件)中、「内容に必要な情報が含まれている」、「内容に関心がある」とする回答がそれぞれ約8割と突出している。また情報提供のタイミング、内容のわかりやすさ、レイアウト、文章の読みやすさに対する肯定的な評価が各々半数を上回った。

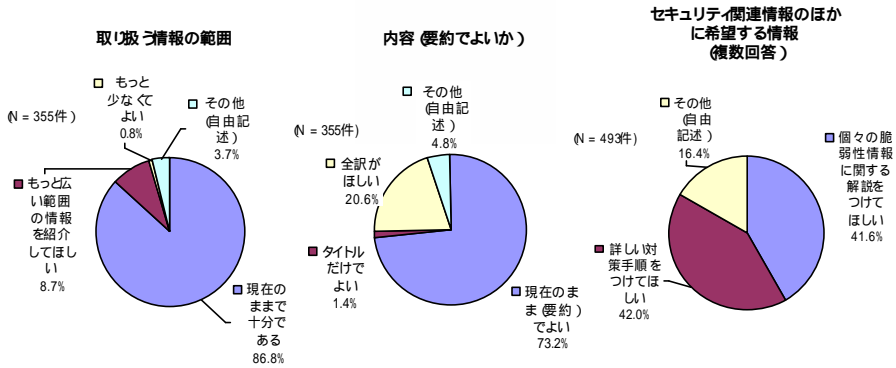
一〇メモについては、肯定的な評価が各項目とも5割から7割と平均している。わかりやすさ、読みやすさについては脆弱性情報よりも肯定的な評価が多い。情報提供のタイミングについて最多回答が「どちらともいえない」となっているが、とりあげている情報が必ずしも脆弱性情報のように緊急性の高いわけではないことを反映しているものと思われる。

JPCERT/CC レポートの内容に対する評価



### JPCERT/CC レポートで取扱う情報の範囲、内容、セキュリティ関連情報のほかに希望する情報

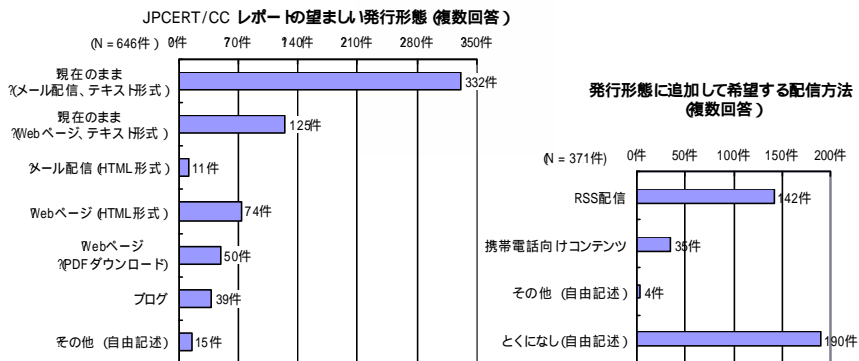
JPCERT/CC レポートで扱う情報の範囲は、「現在のままで十分である」とした回答は全体の86.8%、提供される情報は「要約でよい」とした回答は全体の73.2%であり、現状のままでよいとする評価が大勢を占めた。ほかに希望する情報としては、「個々の脆弱性情報に関する解説」・「詳しい対策手順」が挙げられた。



### JPCERT/CC レポートの望ましい発行形態

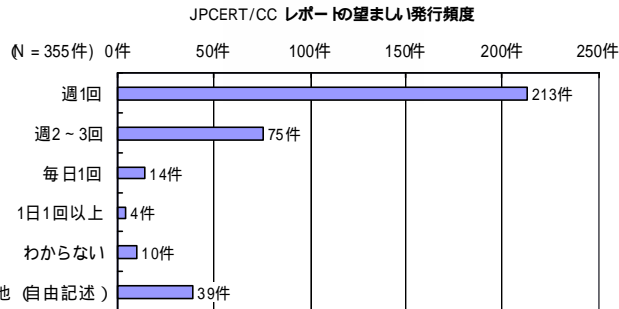
JPCERT/CC レポートの望ましい発行形態については、「現在のまま(メール配信、テキスト形式)」とする回答がほとんどで、全回答件数(655件)中の332件(50.7%)であった。「現在のまま(Webページ、テキスト形式)」とする回答とあわせると、7割以上が現在の発行形態が望ましいと回答した。

また、現在の発行形態に追加して希望する配信方法については、3割程度がRSS配信を希望すると回答した。



### JPCERT/CC レポートの望ましい発行頻度

JPCERT/CC レポートの望ましい発行頻度は現在の発行頻度と同様の「週1回」とした回答が、全回答件数(355件)の約6割を占めた。その他の自由記述意見として基本は週1回でよいが、重要度が高いものは「随時」としたものが20件あったことから、重要度が高い情報を随時で提供している「JPCERT/CC Alert」の位置づけが正しく認知されていない状況もうかがえる。

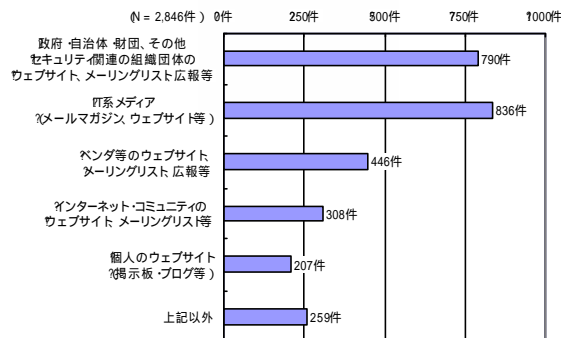


## 2.3 JPCERT/CC以外の、脆弱性情報、インシデント情報の主な入手先

### JPCERT/CC以外の、脆弱性情報、インシデント情報の主な入手先

JPCERT/CC以外の、脆弱性情報、インシデント情報の主な入手先は下記のとおりである。下記の各カテゴリのうち具体的な入手先としてもっとも多かった回答は、それぞれIPA(独立行政法人情報処理推進機構)217件、IT Pro 216件、Microsoft 205件、Slashdot Japan 126件、「セキュリティホールmemo」188件であった。

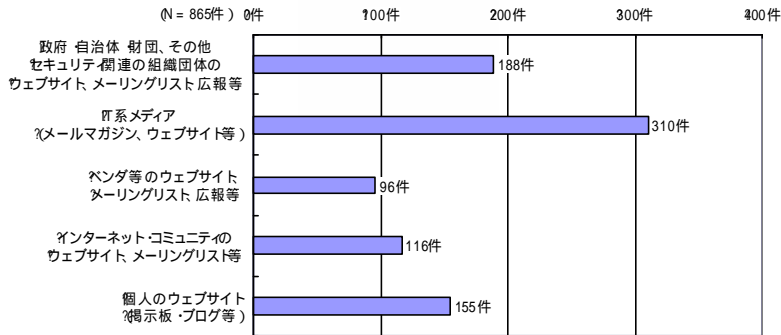
### JPCERT/CC以外の、脆弱性情報、インシデント情報の主な入手先 (複数回答)



### 毎日必ず確認している脆弱性情報源の有無

毎日必ず確認している脆弱性情報源が「ある」とする回答は全回答件数(355件)中210件(59.7%)であり、主な情報源は下記のとおりであった。下記の各カテゴリのうち具体的な入手先としてもっとも多かった回答は、それぞれ「IPA(独立行政法人情報処理推進機構)」46件、「IT Pro」79件、「Microsoft」39件、「Slashdot Japan」56件、「セキュリティホールmemo」138件であった。

毎日必ず確認している脆弱性情報源の有無(複数回答)



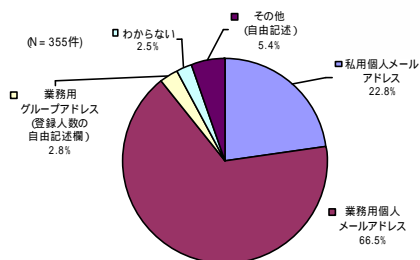
## 2.4 JPCERT/CC レポートの利用期間

### JPCERT/CC レポートを受信するメールアドレス、レポートの利用期間

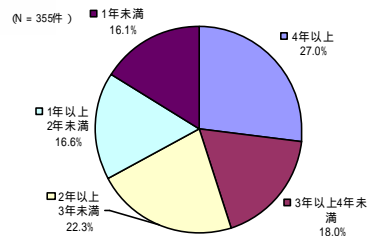
JPCERT/CC レポートは、7割近くの回答が、業務用個人メールアドレスで受信しているとした。JPCERT/CC レポートを他に転送しているとした回答は、全体の6%程度であり、転送先の人数の回答を見ると、10人から100人程度であった。

また、JPCERT/CC レポートの利用期間は4年以上から1年未満までほぼ均等に分散しており、定期的に読者が入れ替わっていることがうかがえる(JPCERT/CC レポートは、2001年6月から発行)。

受信するメールアドレス



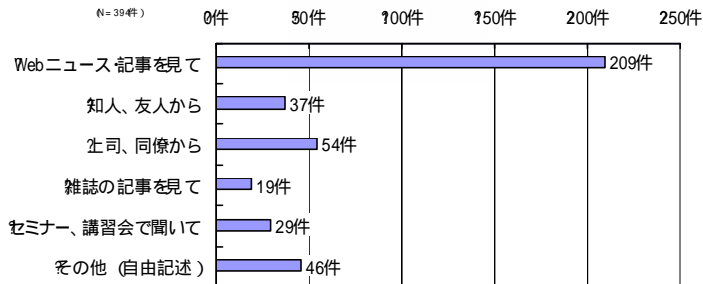
利用期間



### JPCERT/CC レポートを知ったきっかけ

JPCERT/CC レポートを知ったきっかけについて最多数の回答は「Webニュース 記事を見て」としたもので209件あった。「その他」の自由記述では、「JPCERT/CC のWebページで知った」「セキュリティホールmemoで知った」とした回答も見られた。

JPCERT/CC レポートを知ったきっかけ (複数回答)

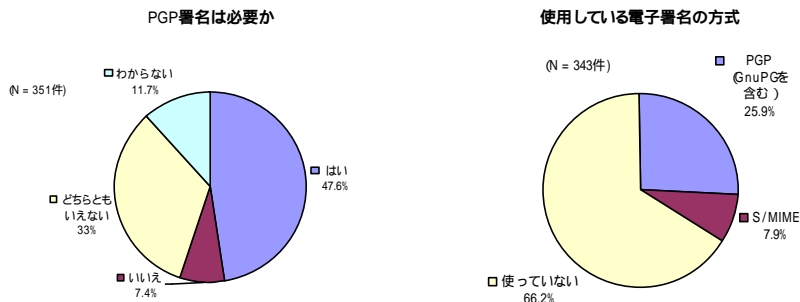


## 2.5 PGP署名について

### PGP署名の必要性、および、使用している電子署名

JPCERT/CC レポートにPGP署名がついていることを知っている、全回答件数 (352件) 中297件 (84.4%) が回答した。PGP署名が必要であると答えた人は約半数を占めた。

また、使用している電子署名としてPGP署名を挙げた人は、25.9%であった。

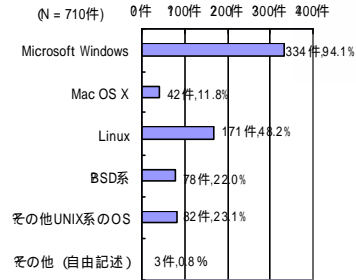


## 2.6 回答者のプロフィール

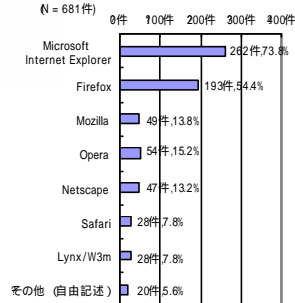
### 普段使用しているOSとWebブラウザの種類

普段使用しているOS、WWWブラウザの最多回答は、それぞれ市場占有率が高いMicrosoft Windows、Microsoft Internet Explorerであった。使用数するOSがWindowsであると回答したのは全回答件数(355件)中334件(94.1%)であり、また、WebブラウザがMicrosoft Internet Explorerとする回答は全回答件数(355件)中262件(73.8%)を占めた。

普段使用しているOSの種類 (複数回答)  
比率は、全回答件数(355件)に対する比率



普段使用している Web ブラウザ (複数回答)  
比率は、全回答件数(355件)に対する比率

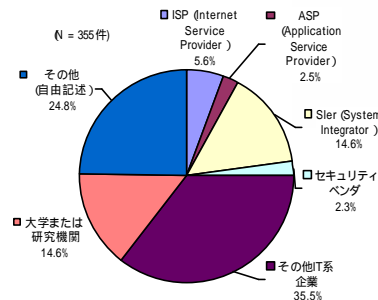


### 所属組織と職種

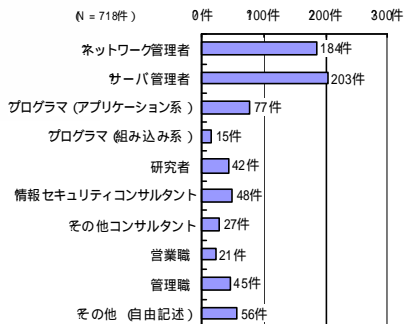
回答者が所属する組織は「その他IT系企業」がもっとも多く、全回答件数(355件)中35.5%を占めた。「SP、ASP、Sler」に所属するとして回答は合計22.7%であった。

職種は、「サーバ管理者」が28.3%、「ネットワーク管理者」が25.6%と突出して多く、どちらも全回答件数(355件)の6割近くを上った。

所属組織



職種 (複数回答)



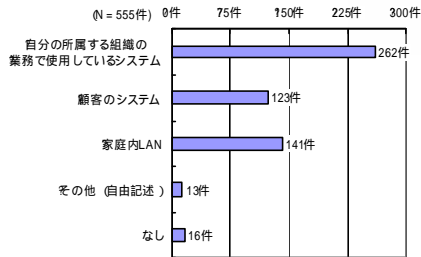


### 管理しているネットワークやサーバの種類、および管理している機器の台数

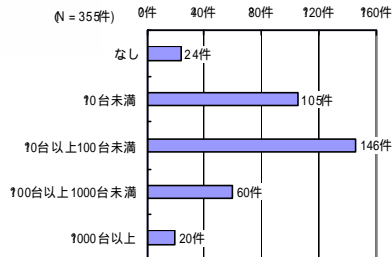
管理しているネットワークやサーバの種類のうち、最多の回答は「自分の所属する組織の業務で使用するシステム」であり、複数回答全回答件数 655 件中 262 件 (47.2%) であった。

セキュリティ対策の対象として管理している機器 (サーバ、クライアントPC、ルータ、L3スイッチなど) の台数は、「10 台以上 100 台未満」とした回答がもっとも多し 146 件 (41.1%)、次いで「10 台未満」とした回答が 105 件 (29.6%) だった。

管理しているネットワークやサーバの種類  
(複数回答)



セキュリティ対策の対象として  
管理している機器の台数



### 勤務地または居住地

勤務地または居住地は、「関東」とした回答は全体の67.0%であり、大多数を占めた。

