

標的型サイバー攻撃への対応について ～参考資料～

平成23年5月27日
経済産業省
商務情報政策局

特定の組織・人を標的として、主として、組織・人の機密情報を詐取等することを目的としたサイバー攻撃。

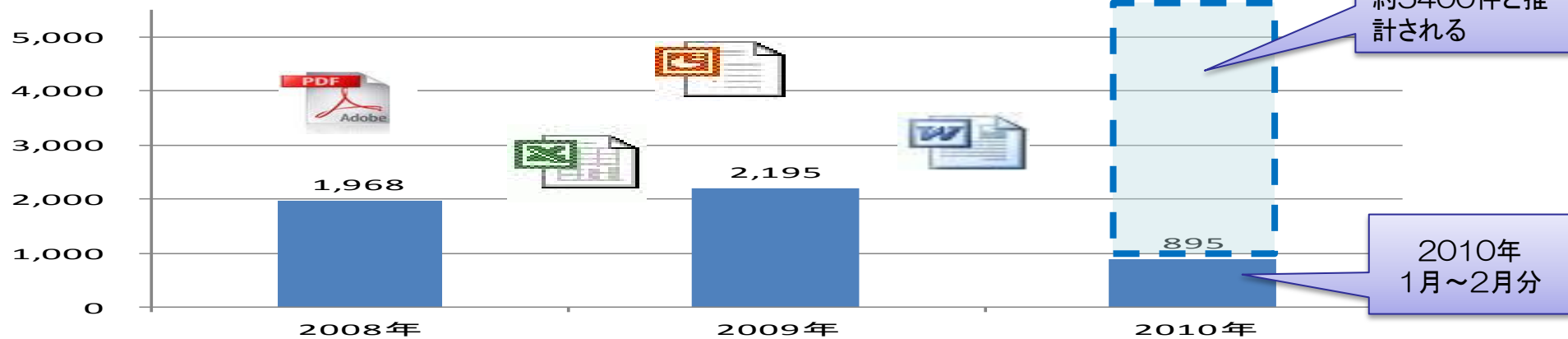
- ① 攻撃の成功率を高めるため、その組織・人を信じ込ませるようにその組織と業務上関係のある組織・人を騙り、あるいは公的機関を装ってメールを送信する等して、そのメールの添付ファイルに情報を窃取等するプログラムを密かに埋め込むなどの手法(ソーシャル・エンジニアリング)を使うことが多い。
- ② 攻撃者がソーシャル・エンジニアリングによらずに攻撃対象の組織・人の使用するITシステム中のセキュリティ上の弱点(ぜい弱性、又は、セキュリティ・ホールという)を直接突いた標的型サイバー攻撃もある。
- ③ 海外では、①のような詐欺的なメールの送信行為を「スピア・フィッシング」又は「ターゲッテッド・フィッシング」と呼んでいる。我が国では、これを一般に「不審メール」と呼んでいる。
- ④ なお、経済的利得や国家機密取得のための秘密情報の窃取・詐取等と関係がなく、情報システムの機能をダウンさせるDoS攻撃やホームページの書き換え等の攻撃は、特定の組織・人物に対する攻撃であっても「標的型サイバー攻撃」とは呼ばない。

1. セキュリティ侵害による知的財産流出の被害額

- 2009年に発表されたマカフィー社の調査によれば、2008年におけるセキュリティ侵害による知的財産流出の1社当たりの平均被害額は以下のとおり。
 - 全業界の平均被害額 460万ドル (約4.8億円)
 - 金融サービス業の平均被害額 530万ドル (約5.5億円)
 - 製造業の平均被害額 460万ドル (約4.8億円)
- ※2008年:104円/ドル
- また、同調査によると、
 - 知的財産がサイバー攻撃の新たな標的になっている。
 - 多くの企業で、情報技術担当はこの問題について弁護士に相談はしない。同じ問題を抱えていることに誰も気づいていない。

出典: マカフィー社「無防備な経済: 重要情報の保護」(2009年)

[欧州の金融機関に対する不正プログラムの埋め込まれた添付ファイル付きの標的型攻撃メールの例]

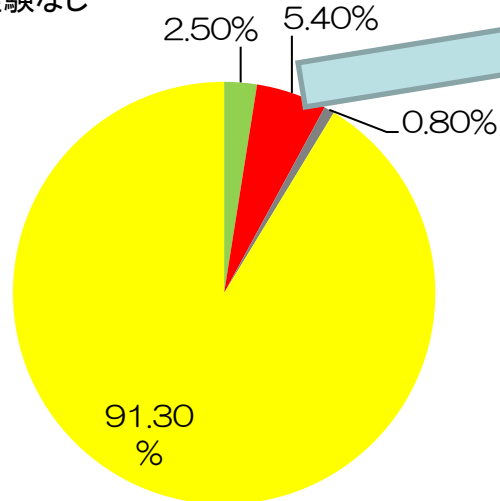


(出典: F-secure のデータをもとに作成。2010年の点線はMETI)

2. 標的型サイバー攻撃に関するユーザアンケートの概要(1)

標的型と思われるサイバー攻撃を受けたことがあるか(2007年)

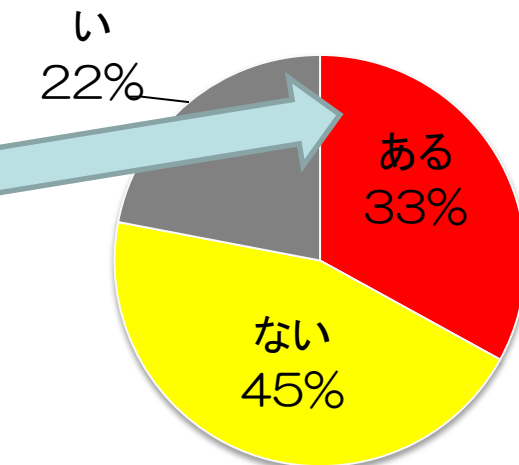
- スピアフィッシング
- 関係者を装った社員宛のウィルスメール
- 「DoSをしかける」という脅迫メール
- 経験なし



出典: 経済産業省委託調査(2007年)

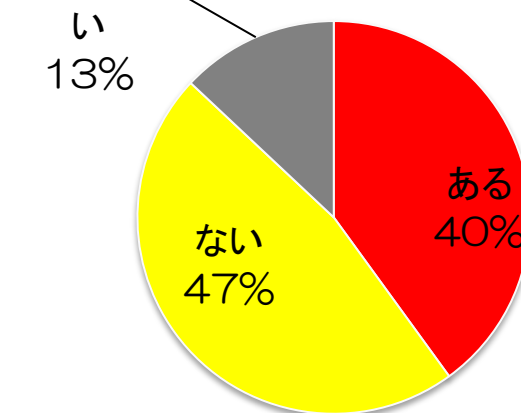
標的型と思われるサイバー攻撃を受けたことがあるか(2011年)

分からない (n=46)



標的型と思われるサイバー攻撃によって不正プログラムに感染したことがあるか

分からない (n=15)

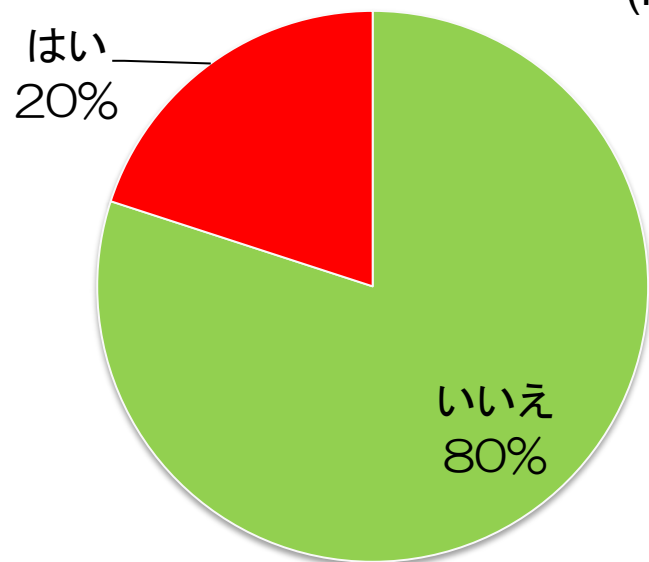


出典: 経済産業省調査(2011年)

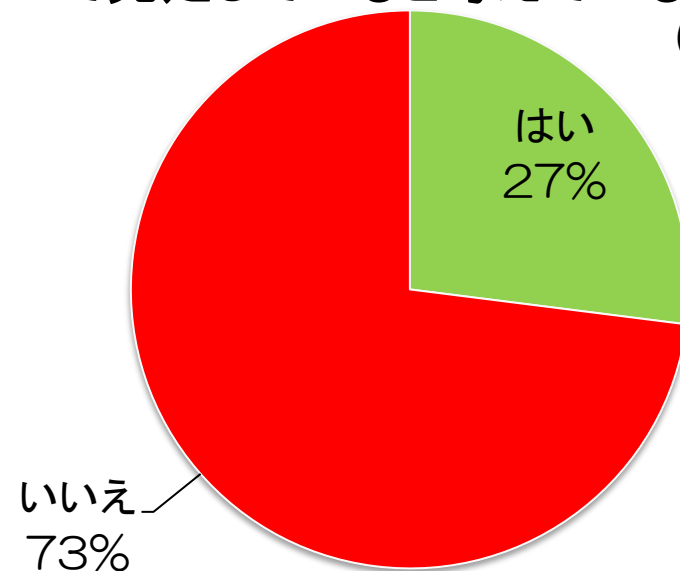
ユーザ企業に対するアンケートを通じ、33%のユーザ企業に対して標的型と思われるサイバー攻撃が行われている実態が確認された。また、標的型と思われるサイバー攻撃を受けた企業の40%が実際に不正プログラムの感染にまで至っていることが確認された。

2. 標的型サイバー攻撃に関するアンケートの概要(2)

標的型と思われるサイバー攻撃によって被害を受けたことがあるか
(n=15)



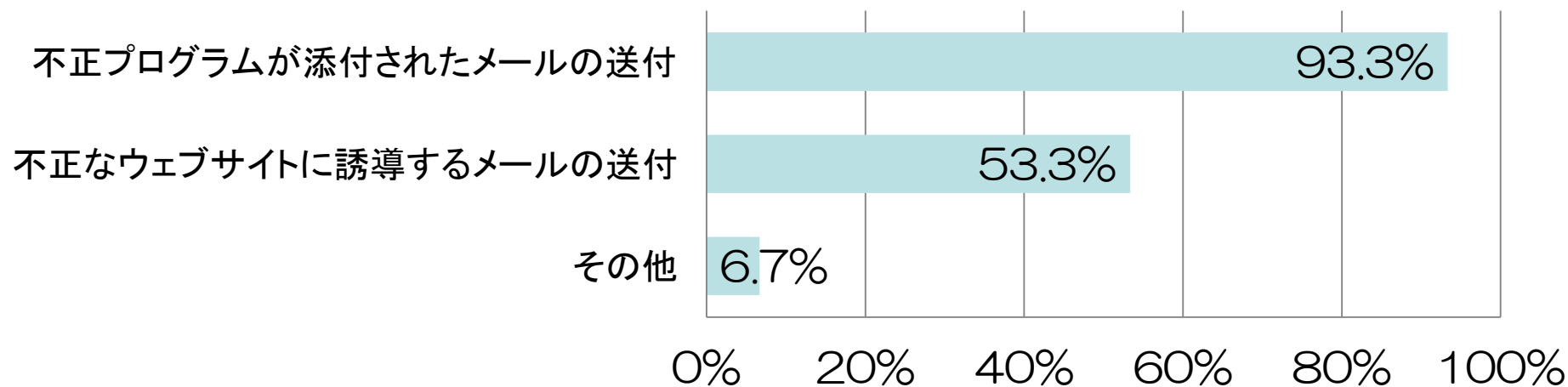
標的型と思われるサイバー攻撃への対応に関し、企業(個社)としての対策で充足していると考えているか
(n=15)



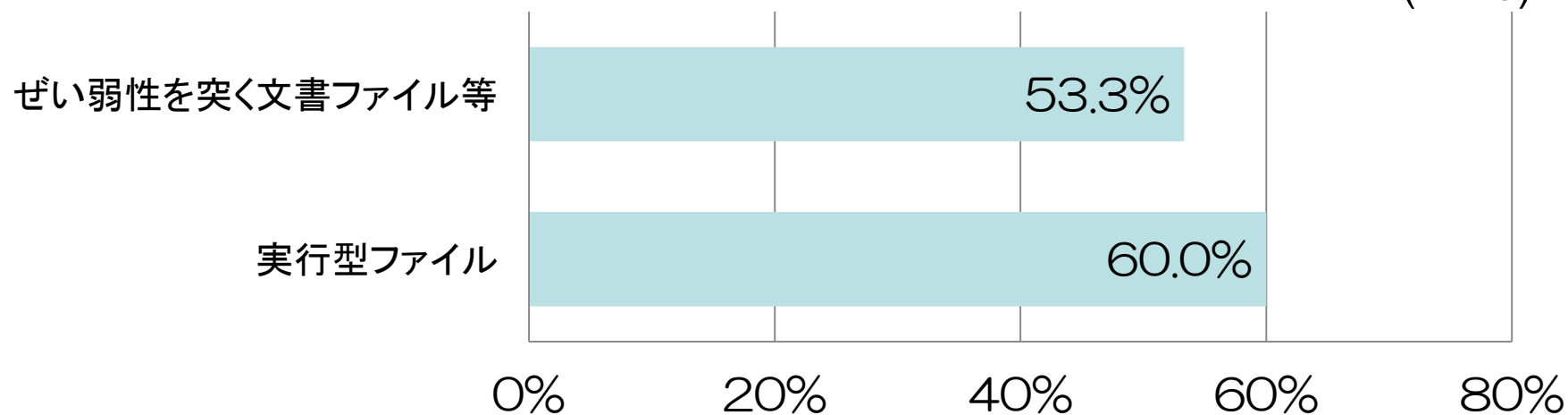
出典: 経済産業省調査(2011年)

2. 標的型サイバー攻撃に関するアンケートの概要(3)

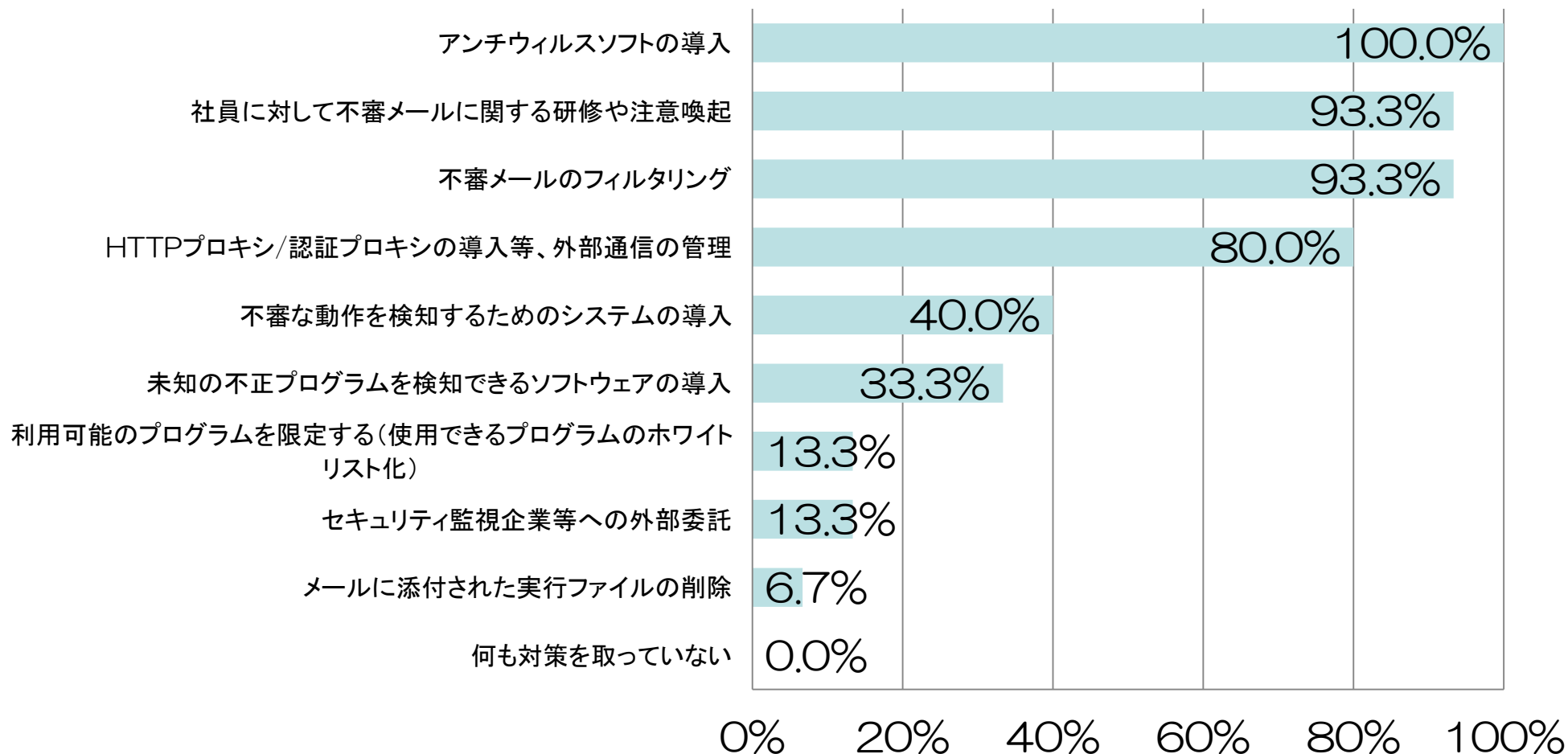
標的型サイバー攻撃に使用された手法【複数回答】 (n=15)



標的型攻撃に使用された不正プログラムの種類【複数回答】 (n=15)



標的型サイバー攻撃に対する対策【複数回答】 (n=15)



出典: 経済産業省調査(2011年)

3. 標的型サイバー攻撃への対応に関する委員の意見

【ユーザの自衛的措置に関する意見】

新委員(東京電機大学)

・現在のアクセスまたはインターフェースによる監視では限界があり、(システムの)正常な振る舞い、異常な振る舞いという形から監視していかなければ対応していくことは困難との印象。

高橋(正)委員(マイクロソフト社)

・動かしてはいけないプログラム(不正プログラム)を検知する考え方から、動かしても大丈夫なプログラムを指定していくという考え方に変えていく必要がある。

鵜飼委員(フォーティーンフォーティ社)

・標的型攻撃のリスクを(システム構築レベルで)軽減していくための取組を進めていく必要がある。

【社会全体としての防御措置に関する意見】

小屋委員(トレンドマイクロ社)

・標的型攻撃は企業の知的財産や機密情報を狙ったものがほとんど。標的型攻撃は今後増加していくと予測。

・社会に対して、攻撃の全体像や効果的な対策を示していく必要がある。

西本委員(ラック社)

・標的型攻撃に関する情報は現在は共有されていない。せめて共有の体制があれば共有が促進されるのではないか。民間事業者で現在情報共有促進を試行している。

・標的型攻撃への対応のためには目的の調査や使用される不正プログラムの解析が必要だが、そのようなことは民間事業者では行わない。

小林委員(倉敷芸術科学大学大学院)

・攻撃手法の使い回しの有無により、情報共有して意味があるものと意味が無いものが出てくる。使い回しの有無にかかわらず、一定の技術対策はありうる。

高倉委員(名古屋大学)

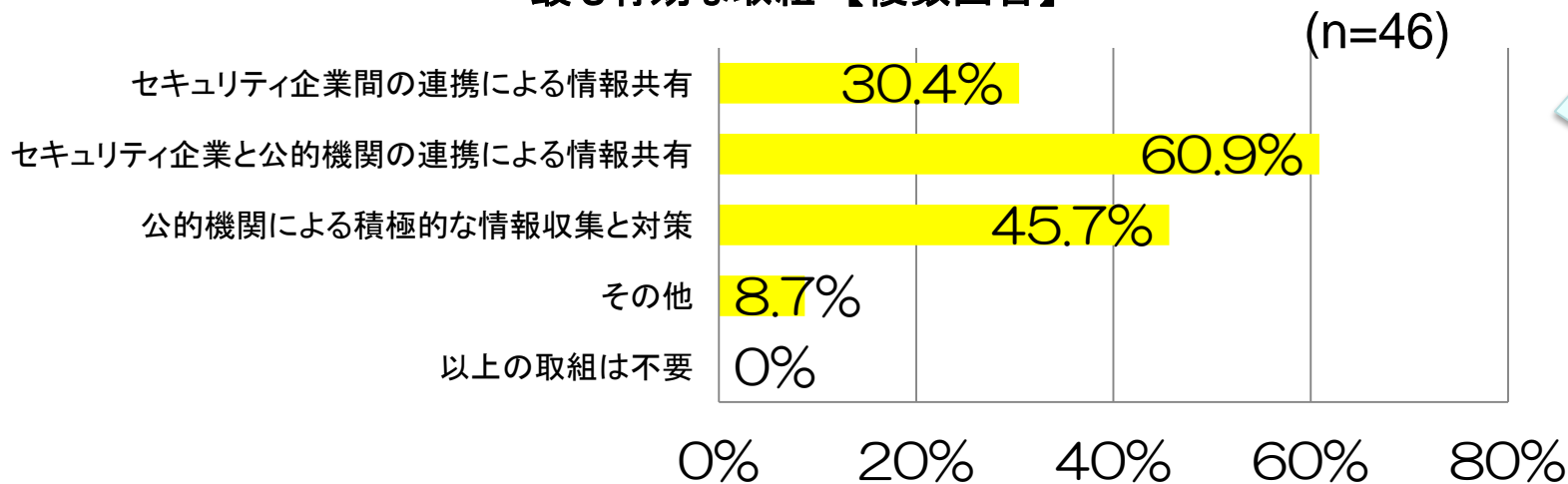
・標的型攻撃は非常に巧妙に行われており、表面的な対応だけでは情報を抜かれてしまう可能性がある。よって、標的型攻撃を受けたら、情報共有を行うことやどこかに相談する必要である。

藤井委員(パナソニック社)

・標的型攻撃の危険性に関する意識がまだ低い。産業界に働きかけ、対策のための情報収集を可能にする環境作りが必要。

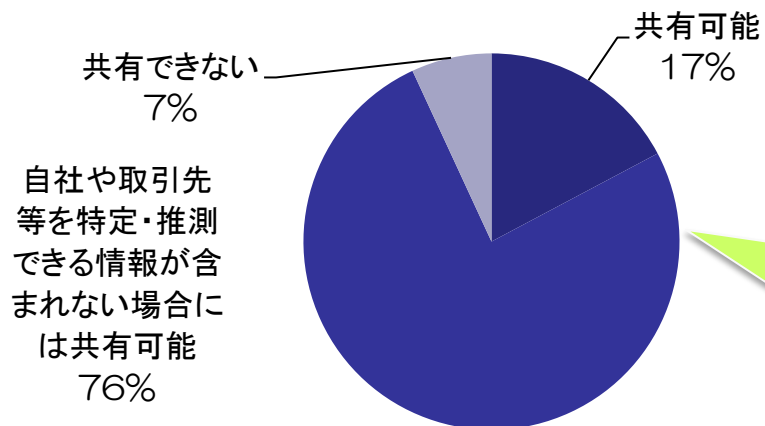
4. 標的型サイバー攻撃に関するアンケートの概要(1)

ユーザが考える標的型サイバー攻撃の被害拡大防止のために
最も有効な取組【複数回答】



ユーザは公的機関が介在した形での取組が有効と考えている。

セキュリティ企業と公的機関の連携取組による
情報共有に関するユーザの考え方 (n=29)

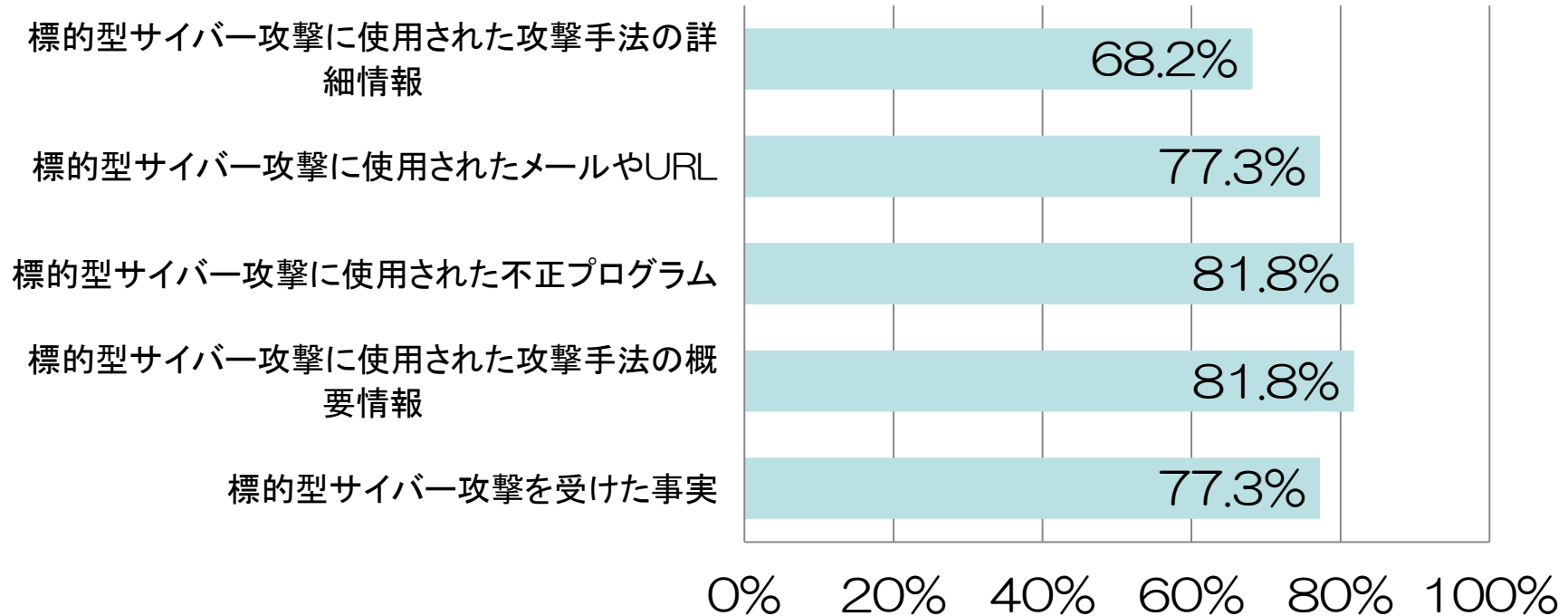


個社を特定できる情報への適切な処理が行われれば、ユーザは情報共有への協力は可能と考えている。

4. 標的型サイバー攻撃に関するアンケートの概要(2)

自社や取引先等を特定・推測できる情報が含まれない場合には
共有可能な情報としてユーザが選択した情報 【複数回答可能】

(n=22)



出典：経済産業省調査(2011年)

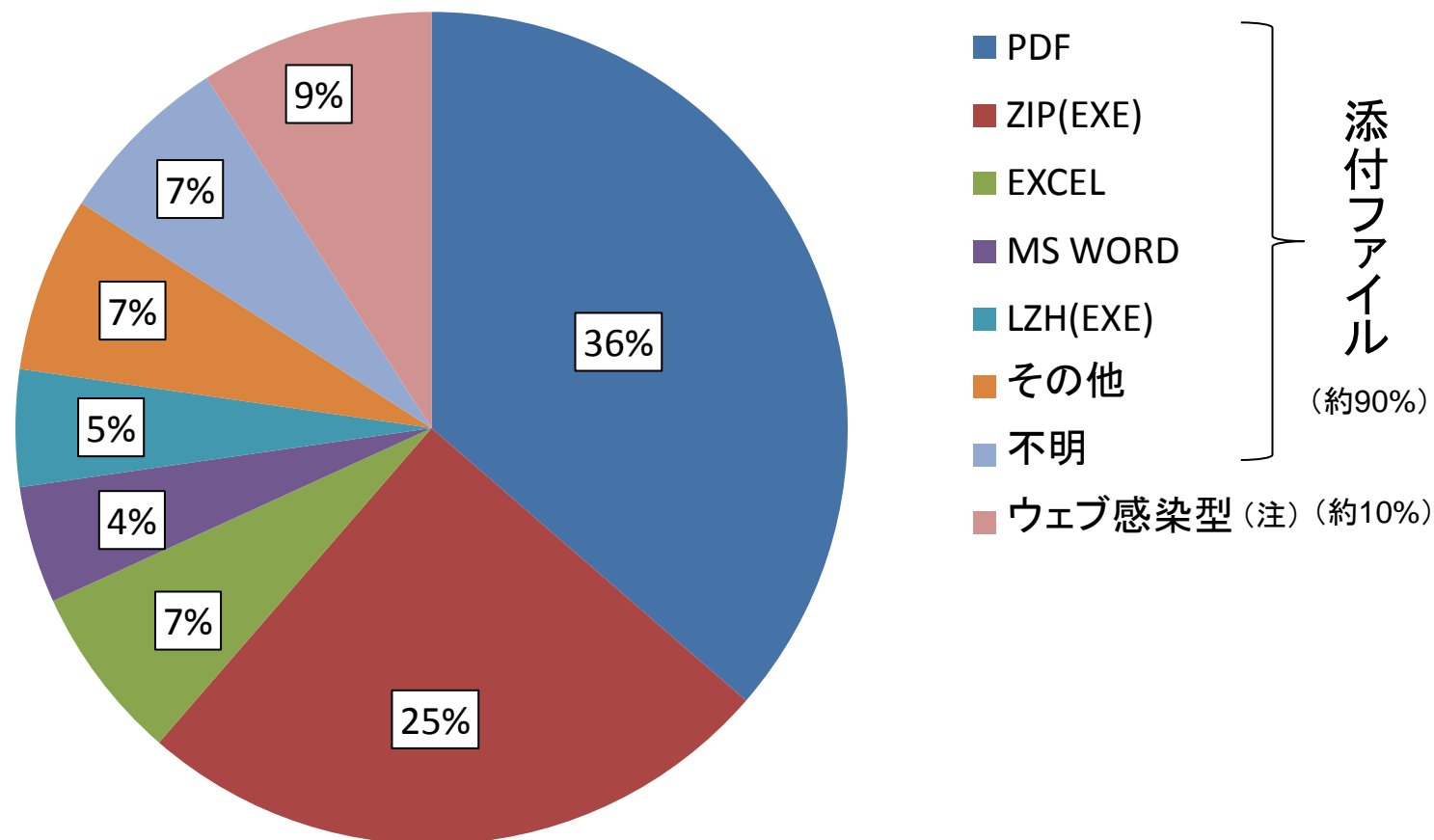
個社を特定できる情報が適切に処理されることを前提に、ユーザは幅広く情報を提供できる用意がある。

- サイバーセキュリティ強化の一環として、米国大統領府はサイバーセキュリティに関する法案を米国議会に提出(本年5月12日)。同法案は、①情報漏えいに関する公的機関への報告、②サイバー犯罪者に対する刑罰の明確化、③重要インフラ分野の防護、④政府機関のセキュリティ強化、を骨子とする内容。
- また、同法案には、サイバー攻撃への対応強化のための任意の情報共有の取組に関する記述。
 - 新たな種類の不正プログラムやサイバーセキュリティ上の脅威を産業界、州政府等が発見した場合、連邦政府への情報共有を円滑にするための取組について提案。
 - 情報提供者の懸念に応えるため、サイバーセキュリティに関する情報提供を行った場合の免責を規定。加えて、任意で提供された情報が個人のプライバシーや市民の権利を侵害しないよう、厳格な管理を行う。

6. 標的型攻撃メールの攻撃手法

(IPAに2008年4月～2010年11月の間に届出られたもの。次頁以降同様)

攻撃手法の種別



(注)メールに記載したURLのウェブサイトに誘導しウイルスに感染させる手法

7. テーマの傾向、主要な時事案件との関係(1)

分類	割合	テーマ事例
イベント	50%	国際会議、シンポジウム、研修会、選挙、法令改正、高官日程、役員人事異動、来訪者情報、社内ウイルス調査
ニュース ・ 注意喚起	30%	金融情勢、国際情勢、外交情報、政府予算、製品事故、情報セキュリティ注意喚起、新型インフルエンザ
報告書	20%	情報セキュリティ調査、ウイルス・不正アクセス届出状況、国際情勢、海外資源、政府部局報告書

7. テーマの傾向、主要な時事案件との関係(2)

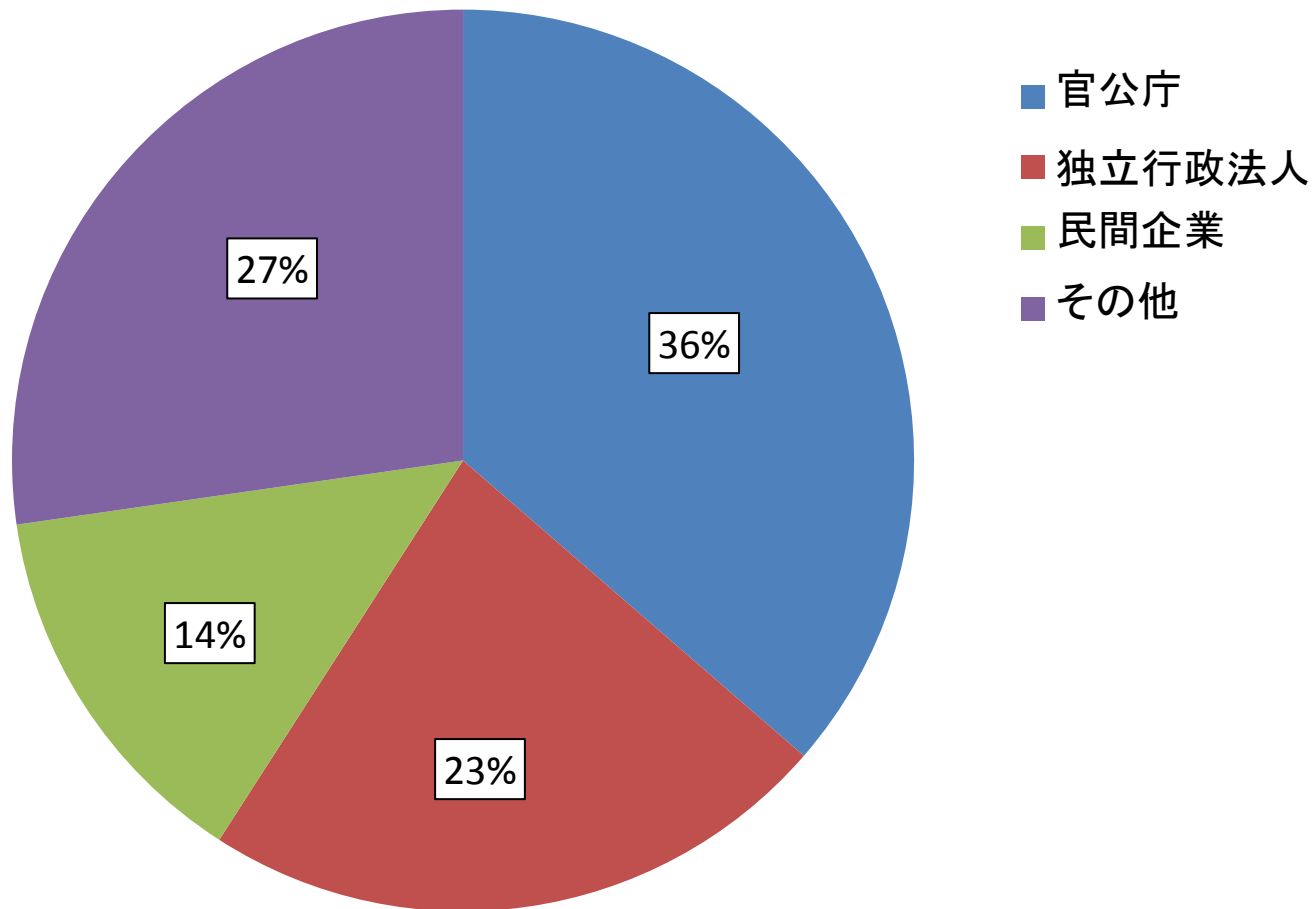
分類	割合	テーマ事例
社会	38%	政府予算、新型インフルエンザ、製品事故、情報流出事故、情報セキュリティ注意喚起、情報セキュリティ調査
国際	34%	国際情勢、国際会議、外交情報、海外資源、外国高官日程
経済	13%	金融情勢、経済関連法改定、経済外交、経済成長戦略
政治	9%	選挙、公職選挙法改正
国内	6%	法人実態調査、高官日程
芸能	0%	

7. テーマの傾向、主要な時事案件との関係(3)

分類	割合	テーマ事例
関係者 限定情報	42%	選挙、演説原稿、法令改定、外交情報、 法人実態調査、海外資源、来訪者情報、 国際会議、高官日程、政府部局報告書、情報流出事故
公開情報	42%	情報セキュリティ注意喚起、情報セキュリティ調査報告、 国際情勢、シンポジウム、金融情勢、経済外交、 新型インフルエンザ、政府予算、製品事故、経済成長戦略
組織内限定	16%	不審メールの注意喚起、社内ウイルス調査、 組織内業務連絡、役員人事異動

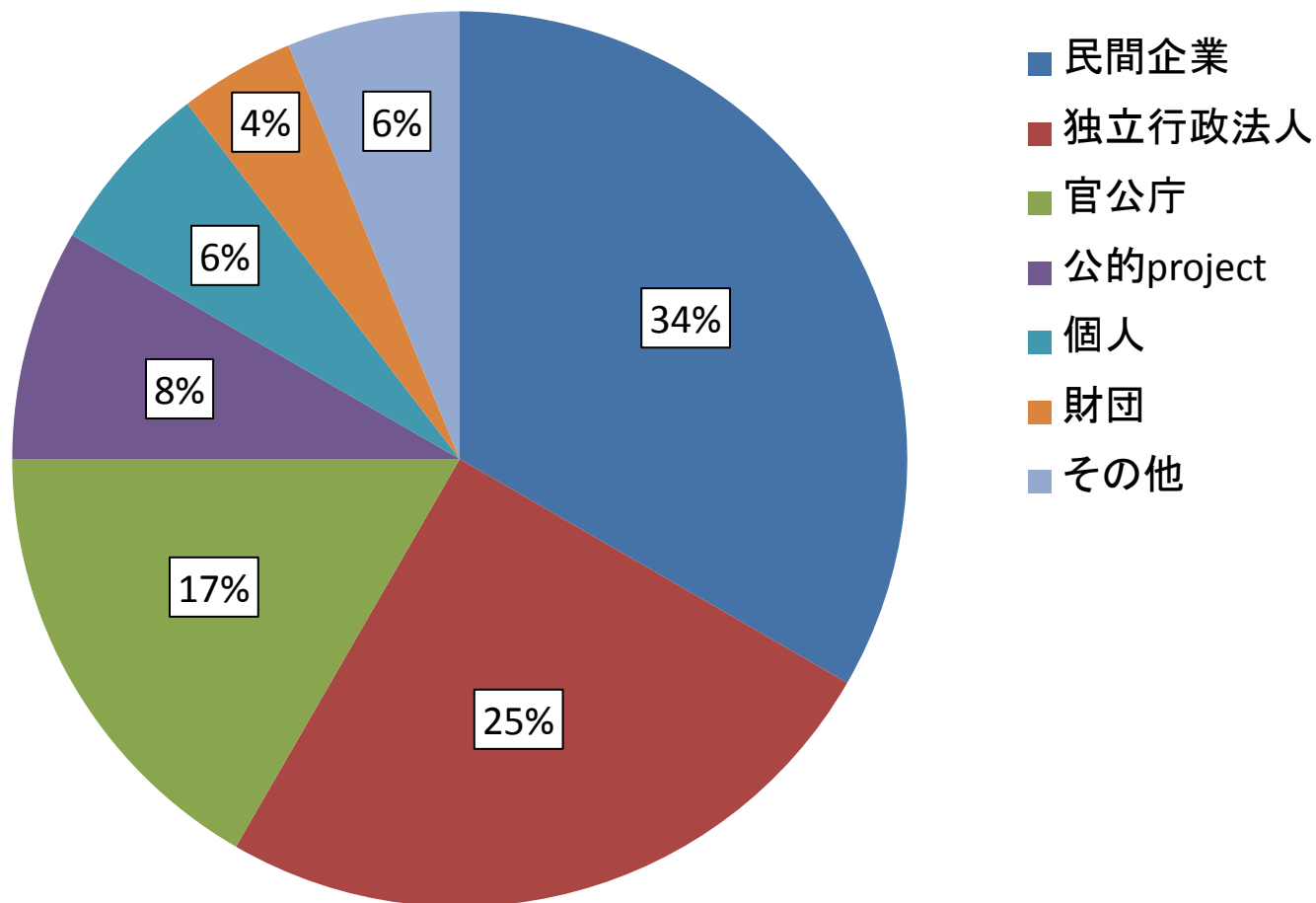
8. 標的型攻撃メール送信者の騙る主体の属性

メール送信者の騙る主体の属性

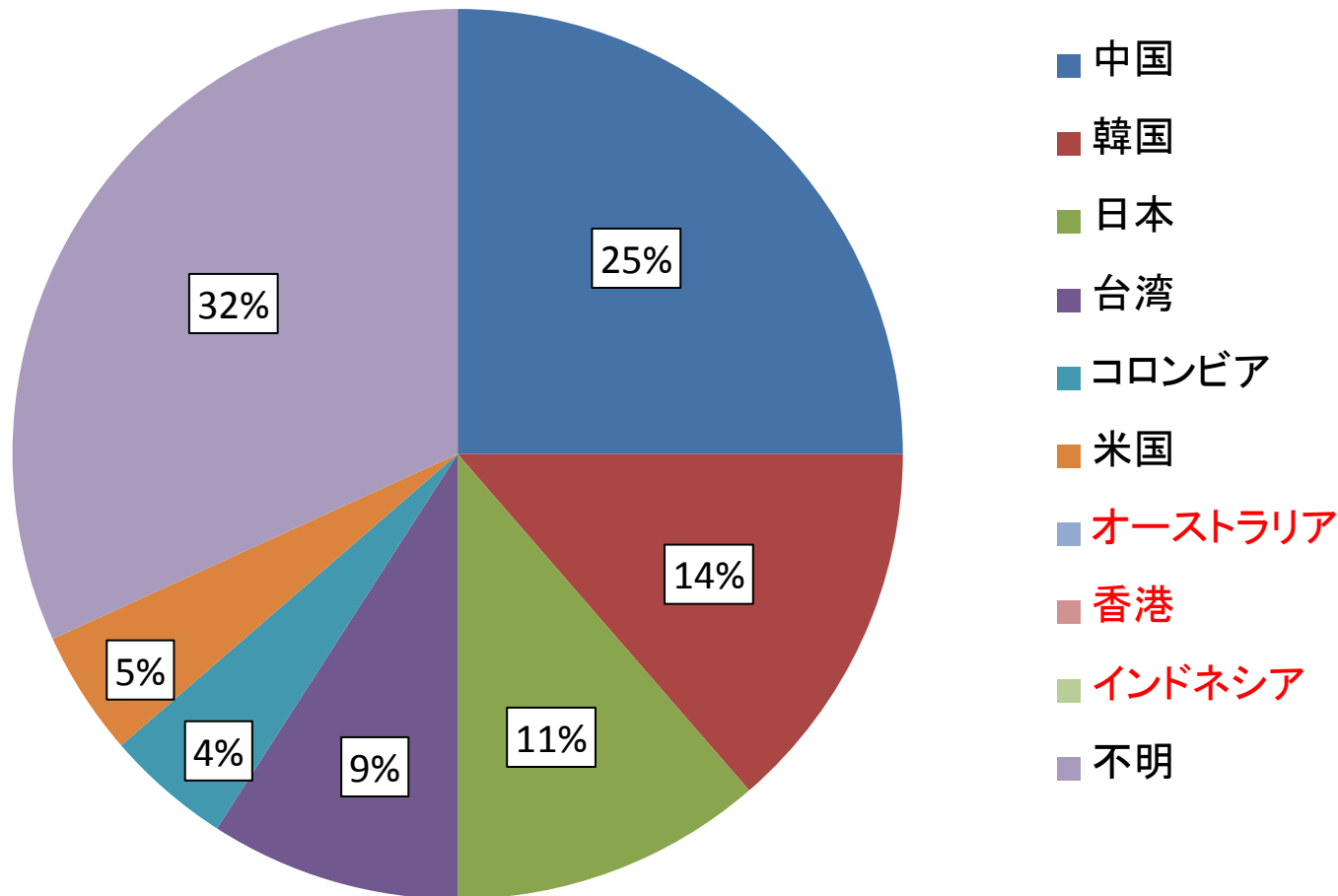


9. 標的型攻撃メール送信先の主体の属性

メール送信先の主体の属性

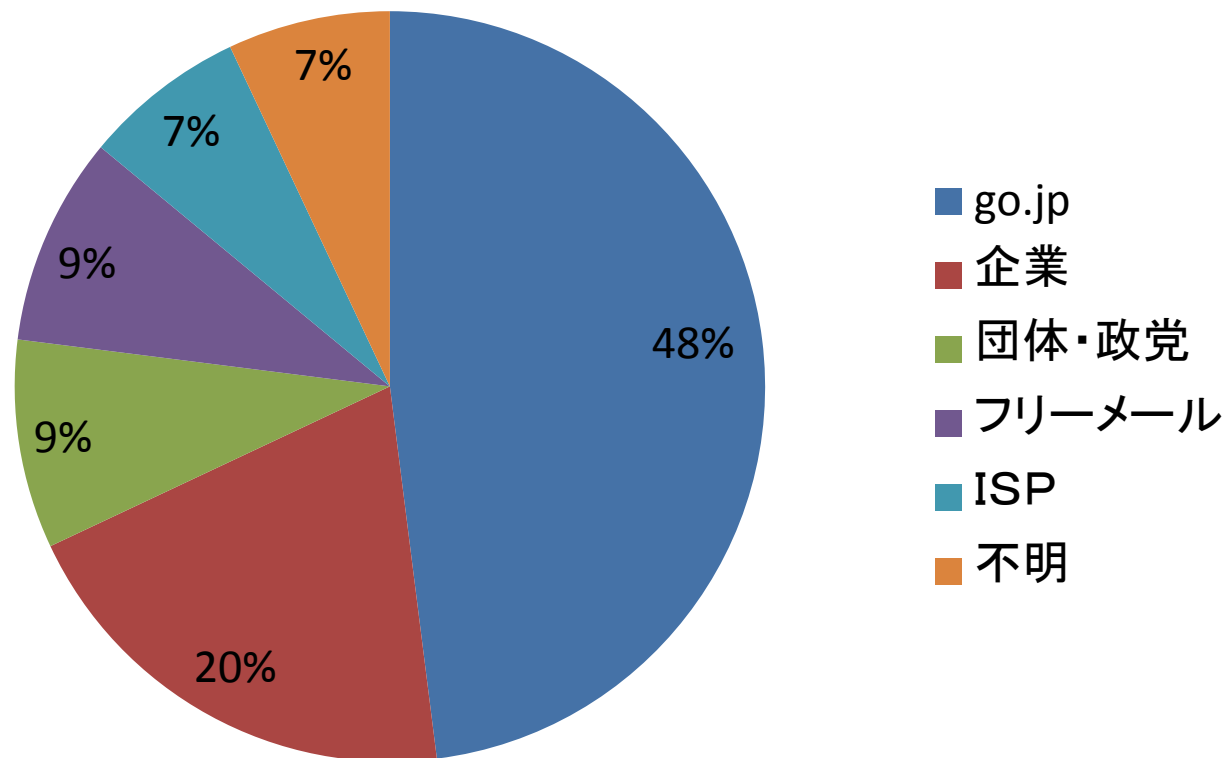


メール発信元IPアドレスの国別の割合



11. (詐称された) 送信元メールアドレスのドメイン

送信元メールアドレスのドメイン



12. 標的型攻撃に悪用された脆弱性があったソフトウェア

標的型攻撃に悪用された脆弱性があったソフトウェア

