別紙

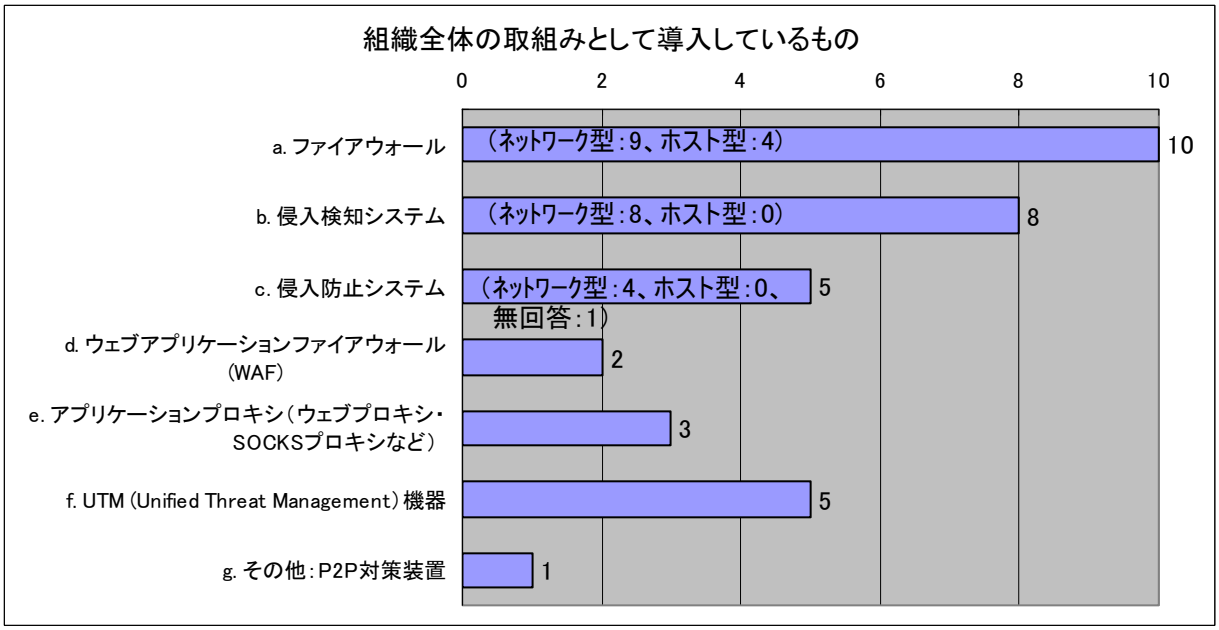
セキュリティ・アンケート 結果

SS 研会員の 10 機関が回答（機関名は A～J で記載）

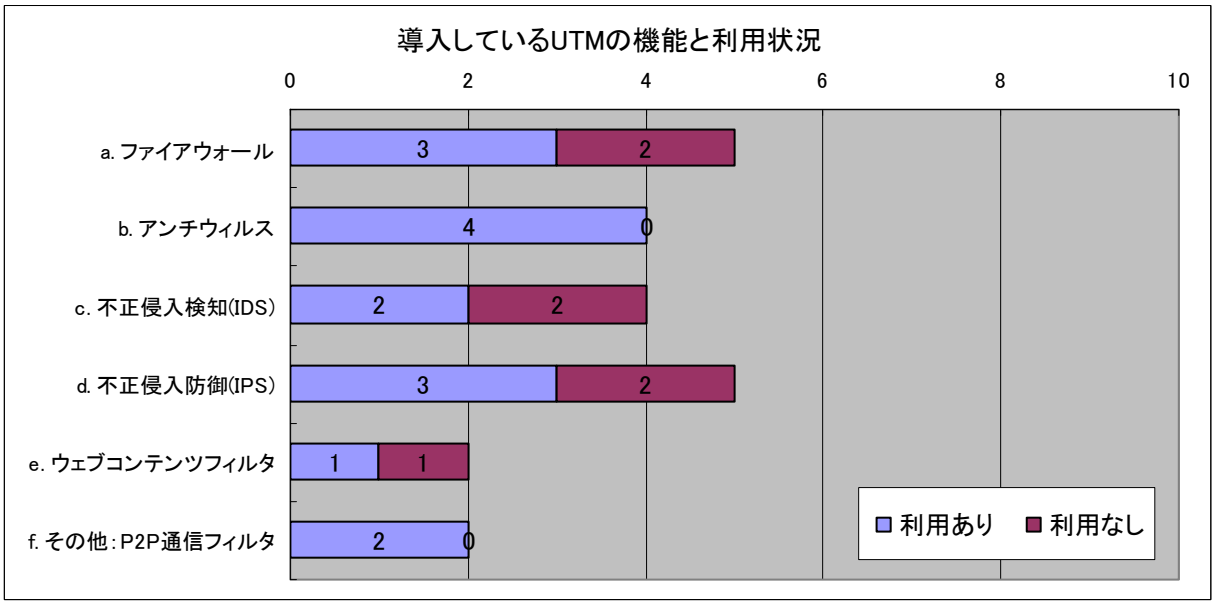
2008 年 10 月実施

Ⅰ．「ファイアウォール、侵入検知・防御装置、ウェブアプリケーションファイアウォールなど」の導入とそのポリシーについて

1. 組織全体の取り組みとして導入しているものは何ですか（複数回答可）



2. UTM を導入している組織は、その機器の有する機能と利用している機能は何ですか（複数回答可）



3. 1.や 2.で回答した機器を導入することになった経緯を、差し支えない範囲で教えてください

- 増加の一途をたどり、かつ巧妙化する情報セキュリティの脅威から、当組織の情報システムを可能な限り保護するため。(A)
- 当初より必要な機器として検討。(B)
- smurf 攻撃をうけて上流のネットワークに迷惑をかけるというセキュリティインシデントが発生したことを契機に IDS を導入した（1998 年度)。続いて、補正予算などでネットワークの再構築をした時に、それまでルータで行っていたアクセス制限をファイアウォールで行うよう変更した（2002 年度頃)。Windows パソコンにウィルスが多発したので、ウィルスのネットワーク通過をできるだけ押さえられるようにウィルスブロック装置として UTM を導入した（2005 年度)。当組織が運用するネットワークに属する大学でワーム感染/不正侵入が発生したので、IDS/IPS を導入した。パーソナルファイアウォールソフトとアンチウィルスソフトをまとめて購入し申請者に無料で配布している。現在は、パソコンの OS にファイアウォール機能が含まれるようになっているので、アンチウィルスソフトのみを導入する方のほうが多い。(C)
- 外部からの侵入を伴うセキュリティインシデントが多発したことによる。(D)
- IDS については、2001 年度末頃に業者からデモ機を借りて評価する機会があった。評価の結果、様々なイベントを見ることができることが分かったため、導入することになったと記憶している。パーソナルファイアウォールは、大手製品を一括ライセンスにより構成員に安価で提供しているものである。導入は必須ではなく、詳しい導入状況は把握されていないのではないかと思う。(E)
- FW/IDS については 2002 年に組織内 LAN をギガビット化した際に、組織内的に FW/IDS 導入の要望があり導入された。FW や IDS の導入の背景については、2001 年～2002 年にかけて行われた、政府省庁に対する攻撃が直接の原因となっている。また 2002 年当時、情報セキュリティポリシーの策定時に、組織内 LAN におけるリスクを知るため IDS を導入することにした。IPS と P2P ファイル共有ネットワークの帯域制御装置として UTM が導入された。(F)
- FW はネットワーク整備時（2001 年）から導入している。P2P 対策は、対応のコストが大きくなったので、ソリューションの提案を受け、導入した。(G)
- 当初から、外部から内部へのネットワークアクセスを制限するために導入している。(H)
- 組織外からの不正アクセスを防止する為。(I)
- 外部からの攻撃が増大したため。(J)

4. 導入して良かったことは何ですか（セキュリティ的な観点と、運用の観点から）

- 事案等の早期発見、早期対応が可能になるとともに、傾向分析が可能となった。(A)
- 問題ある通信や機器を的確に検知している。(B)
- IDS で数多くのセキュリティインシデントを発見できた。また、IDS によるインシデント通信のスナップショット保存機能により完全ではないが、事実関係をある程度正確に把握できるようになった。(C)
- FW を導入して DMZ を構築/運用できたこと。ルータでも可能だが、DMZ の機器毎に細かいアクセスポリシーをルータで設定するのは運用コストが高すぎる。(C)
- 無防備な wireless PC のウィルス/ワーム感染をある程度防御できた。(C)
- FW を導入して不要な通信が遮断できることが実感できたこと、外部からの侵入が減少したこと。(D)
- IDS は監視装置なので、それ自体で何かが直接守れるわけではないが、それまでトラフィック監視についてはスニッファがあるくらいで何が起こってもほとんど調べようがなかったのが、IDS の導入に伴いパケットキャプチャできる環境が整った事で、見えなかったものが見えるようになり、対処できるようになった。外からの攻撃よりも、中からの異常を検出して対処できるようになった事の方が大きいように思う。(E)
- より具体的にこれこれの攻撃を受けているとか、出しているという傾向がわかる事から、その

他のセキュリティ対策の方針決め等にも影響があったものと思う。(E)

- 具体的な攻撃事例などが集まるため、講習会等で説明する際の説得力が増したと思う。(E)
- FW や IDS を導入前後の変化は感じられなかった。IDS については多量のアラートログが得られ、その主成分がポートスキャンであることが判明した。この傾向は、現在も変わらない。P2P ファイル共有帯域制御のおかげで P2P ファイル共有絡みのインシデントはまだ経験していない。一方 IPS を導入したことで、一部サービスの提供に不具合が生じた。(F)
- セキュリティインシデントの回数が減り、コスト削減となった。(G)
- 内部にあるサーバのセキュリティ対策を緩和できる。(H)
- 組織内ネットワークが守られているという安心感。(I)
- 組織内でのウィルス感染件数が減少した。(J)

5. **導入して大変だったことは何ですか(セキュリティ的な観点と、運用の観点から)**

- セキュリティ関連機器がブラックボックス化され、機器の不具合対応等(事案か機器の不具合かの判別を含め)に時間を要してしまう。(A)
- マニアルが不備。マニアルにない設定をしないと、当方の構成では動作しない。(B)
- ネットワーク機器と比較すると購入価格と保守費が高い。(C)
- H.323 通信(TV 会議通信)に障害が発生しやすくきり分けが難しい。(C)
- インシデントの移り変わりもあり、常に陳腐化を心配していないといけない。(C)
- 設定ポリシーの周知が大変だった。また、IDS のログを精査する時間がとれていないこと(事後追跡に使用)。(D)
- IDS の利用方法には業務の方々にも伝えては見たものの、事実上教員が一人で見ている状態で、あまりきちんと監視できていない部分がある。(E)
- 導入から時間が経ってしまい、機器もソフトウェアも陳腐化してしまった。サポートもあって無いような状態になっているが、基幹ネットワークは 10GbE に高速化してしまっていて、それに対応した機器は高価すぎて導入できず、だましだまし使っている状態にある。(E)
- FW/IDS の導入については、情報セキュリティポリシーを策定するにあたり、それらの導入自体が必要事項であったため、ポリシー策定時に必要なリスク分析が可能となり、良かったと思われる。(F)
- 導入後多量のインシデントがあり、とにかく組織が攻撃にさらされている状況を訴えるのには良い資料提供マシンとなった。しかし組織への攻撃のポートスキャンがあまりにも多く、また IDS 設定用の GUI が不安定だったため使い勝手があまりにも悪いこともあり、ログ収集マシンとなってしまった。(F)
- 2003 年当時はログ解析技術があまり普及していなかったので高い投資になってしまった感がある。一方でログ解析技術がこれから有望であることは判ったのはよかったと思われる。(F)
- 独自ポリシーを主張する部署があり、別扱いをしなければならない。(G)
- 内部にあるサーバを外部へ公開する際に不便を感じる。(H)
- ルール定義の組織内調整。(I)
- 初期設定とその手直しが落ち着くまでしばらく大変。(J)

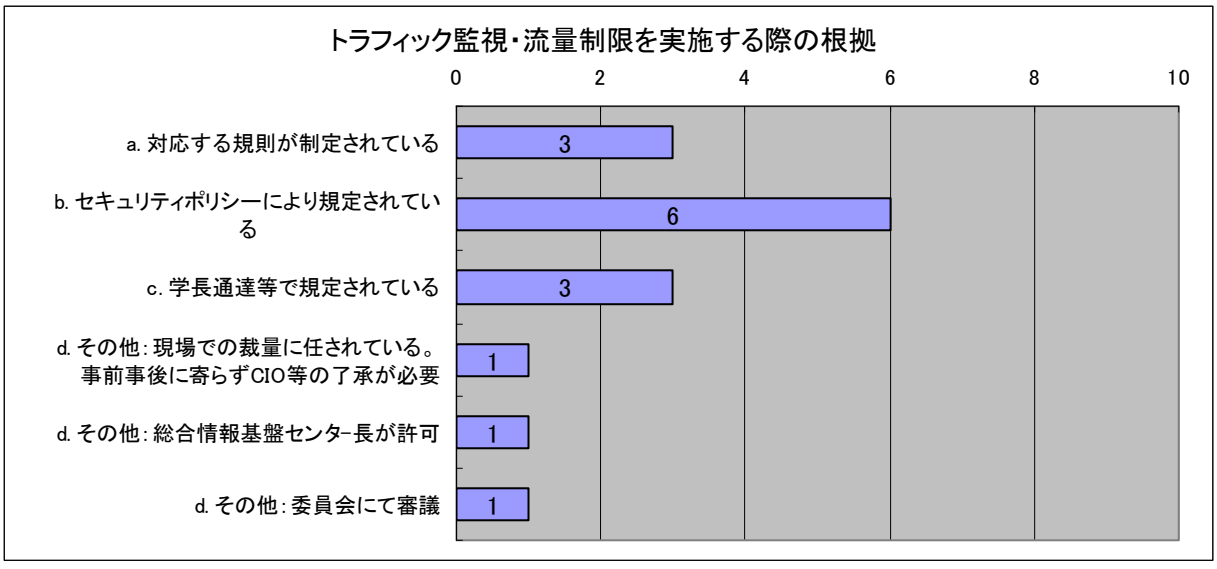
6. **ファイアウォール、IDS/IPS などのさまざまなログをどのように扱かっていますか(長期保存や閲覧規則など)**

- 保存期間はログの種別によって保存期間を定めている(最長 1 年間)。閲覧規則は対応する規程に定められた閲覧者のみ閲覧。(A)
- 現状検索が容易なように DB 化している。今後は外部解析委託を検討。保存としては、アクセス制限はしているが、暗号化などはしていない。保存期間については未決定。(B)
- IDS のログ: IDS のログ解析をアウトソースしているので、アウトソース先と VPN を構築し

常時ログを転送している。(C)

- FW のログ：　syslog サーバへ保存するとともに WLEF 形式を取り扱えるログ解析サーバへも保存し、商用の解析ソフトで解析している。ログとり用の専用のネットワークを構成している。syslog サーバへ保存したログは RAID0+1 の外部ディスクへも保存している。(C)
- 保存：　ログの保存期間は 6 ヶ月以上としている。syslog サーバへ保存したログは、センターが運用する大規模ファイルサーバへ暗号化して保存している。これはバックアップとして考えている。(C)
- 閲覧：　閲覧は、センターのセキュリティ担当者、ネットワークサポート業務受託者、IDS ログの解析のアウトソース先の会社に限定している。(C)
- アクセスが限定された syslog サーバに保存。過去は DVD-R に保存していたが、今は、ある期間後消去。(D)
- IDS はその機器の吐くフォーマットのまま、古いものは別のホストに移して長期保存している。機器固有のファイル形式だが、展開用の Perl スクリプトが提供されており、移しても検索等は可能となっている。基本的に移したものは管理している教員しか見る事ができない状態になってしまっている。(E)
- ログについては情報セキュリティポリシーにおいて記述があり、レガシーな機器を除きログが採れるようにしている。またログなどの閲覧については許可制であり、例えば新種のウィルスに感染した機器については、センター長へ申請して許可を得なければ閲覧できないようになっている。なお研究や業務などでログを常時閲覧する必要がある場合についても、新規の場合については、センター長の許可を得る必要がある。(F)
- ディスク容量の制限のため、短期間保有に限っている。インシデント発生時のみ、センター長の指示により担当者が閲覧する。(G)
- １年間保存し、管理者しかアクセスできないようにしている。(H)
- syslog サーバに送信(保存期間 1 年間)。(I)
- 一定期間保存、管理グループのみで閲覧可能。(J)

7. **トラフィックの監視や流量制限を実施する際の根拠はどのようなものですか**



8. **ログや IDS で収集された通信内容には、通信の秘密やプライバシー等のセンシティブな情報が含まれている可能性がありますが、これら情報の扱いはどのような権限で行われていますか**

- 当組織のセキュリティ関連規程に基づき取り扱っている。(A)
- 未整備。(B)
- 「統計的な処理はするが、通常はログの詳細はみない」、「セキュリティインシデントがあれば、

詳細な内容までみる」という方針で、関係者だけがログをみることができるようにしている。(C)

- 権限は特に定義されていないが、セキュリティポリシーによりインシデント発生時にはその原因を突き止めるためにトラフィック調査をしてよい事になっている。(E)
- 研究や侵入検知業務以外の業務以外では、重要なネットワーク接続機器のログについてはセンター長の許可がなければ閲覧してはいけないことになっている。個人情報であると判断されれば、個人情報保護に関する組織内規定で対応される。(F)
- インシデント時にセンター長の示により担当者が閲覧するように制限している。また、その他の目的の場合には、文書により依頼をし、センター長が決済する。(G)
- Web ページにて、トラブルが発生した際にログデータをもとに情報取得を行う旨通知している。(H)
- 委員会からの要請のみ確認。(I)
- 通信内容はセキュリティ管理上必要な作業(トラブル原因追求)のために管理者のみが参照し、それ以外には公開しない。(J)

9. **1.であげた機器のうち、以前導入していたが運用をやめた機器があれば、その種類と理由を教えてください**

●ホスト型の IDS （A）

理由： ・運用・管理コスト(費用)増大のため

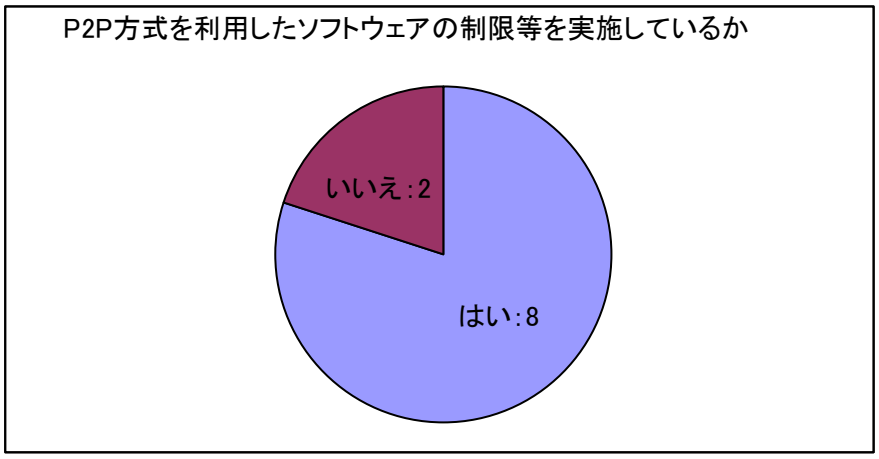
・運用・管理する人員が確保できなくなったため

●ファイウォールソフト （C）

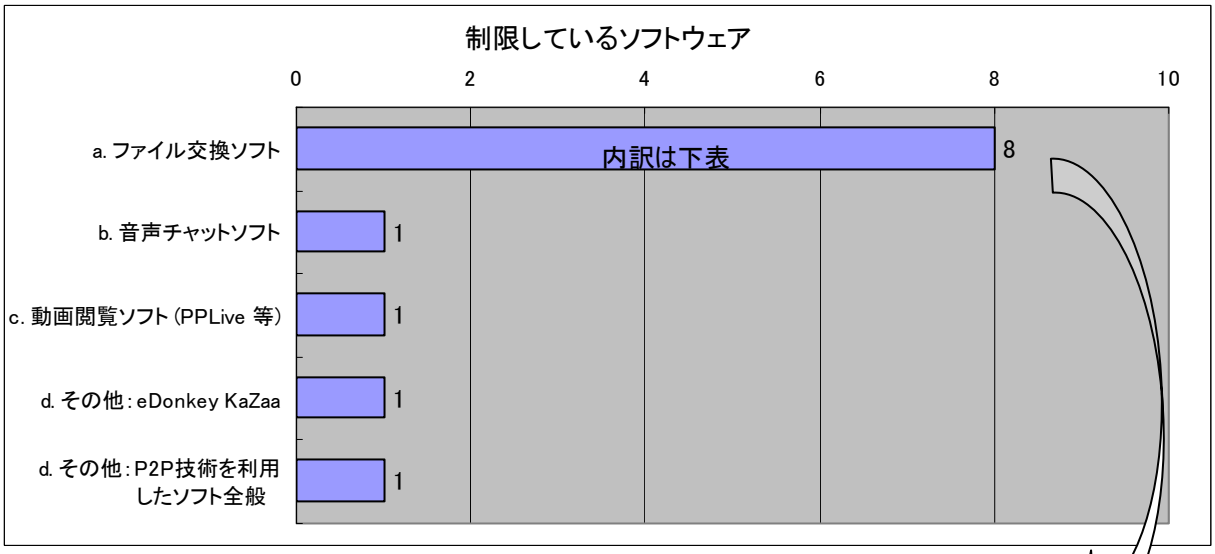
理由： ・機器のメーカーサポートが終了し保守できなくなったため

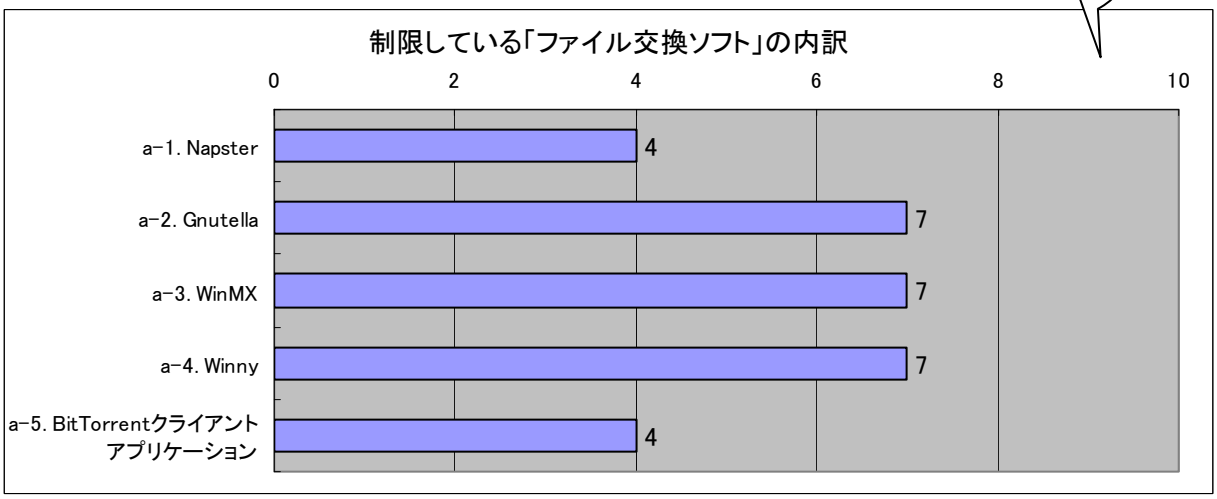
Ⅱ．「P2P」関連ソフトウェアに関する対策とそのポリシーについて

1.　P2P 方式を利用したソフトウェアの制限等を実施していますか

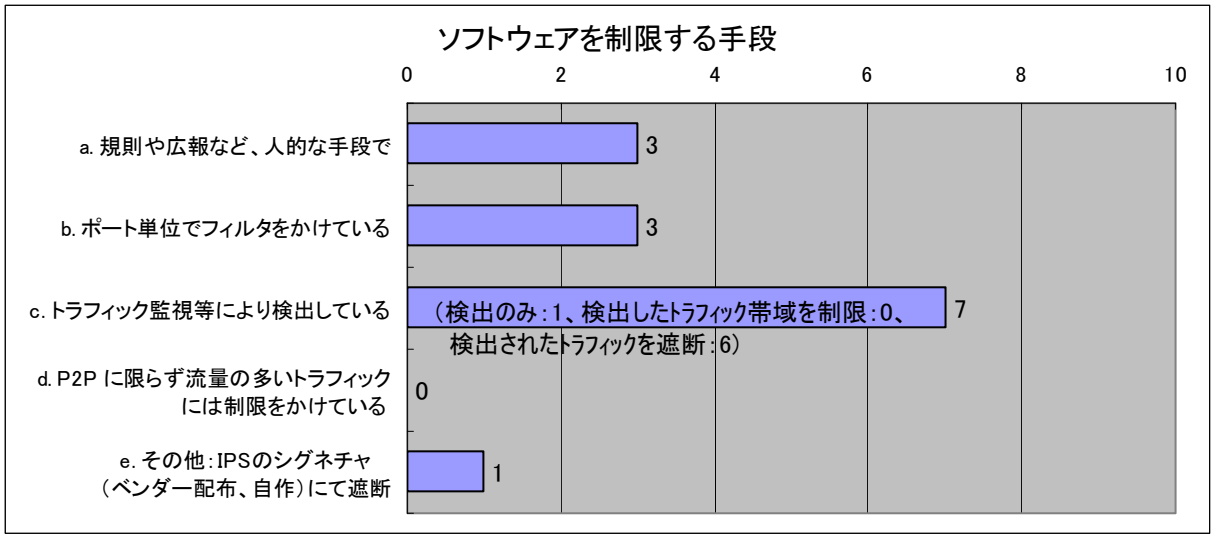


2.　どのような種類のソフトウェアを制限していますか（複数回答可）

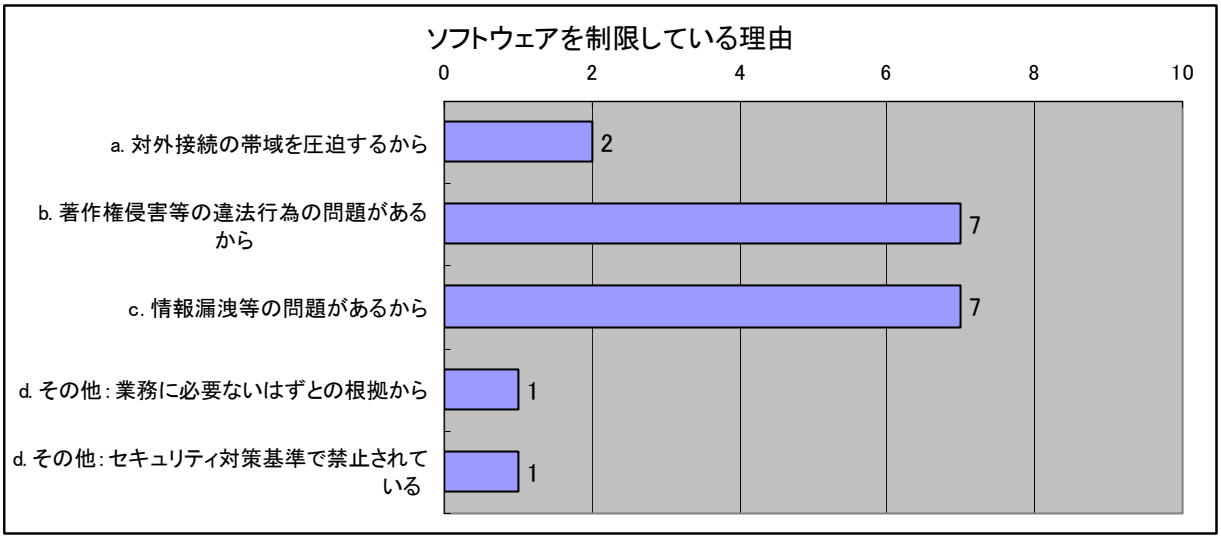




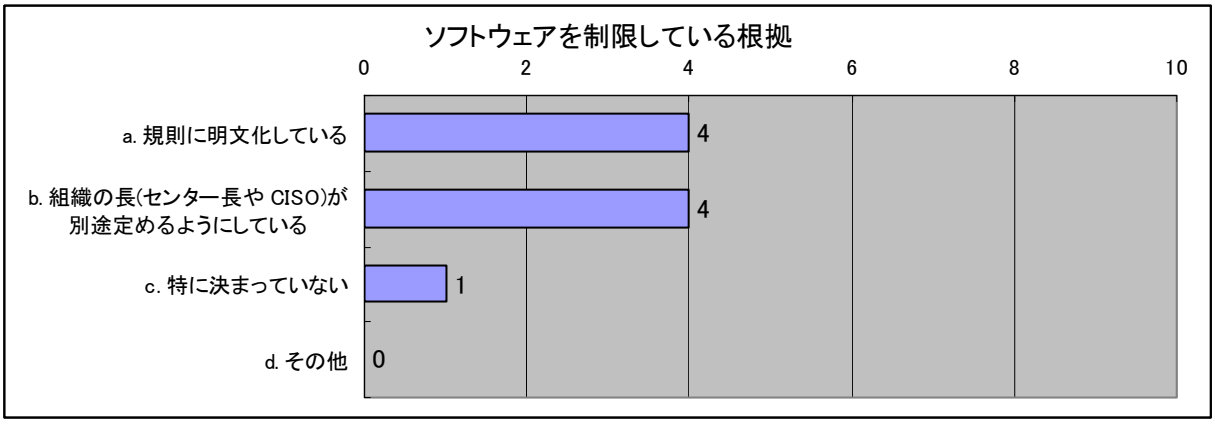
3. 制限する手段はどのようなものですか（複数回答可）



4. 制限している理由を、差し支えない範囲で教えてください（複数回答可）



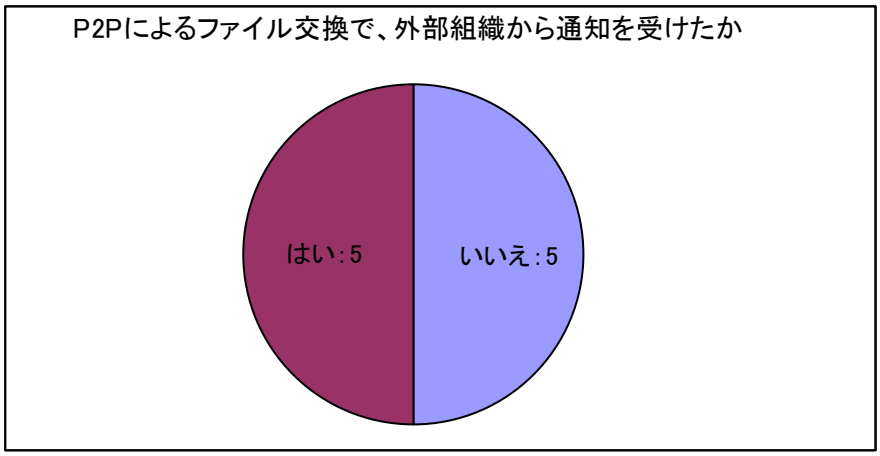
5. 制限の根拠はどのようなものですか（複数回答可）



6. P2P 関連ソフトウェアへの制限等を実施していない理由は何ですか

a. 実施が技術的に困難だから	0
b. 制度的な整備が困難だから	1
c. 導入予算がないから	0
d. 必要性を感じないから	1
e. その他	0

7. P2P によるファイル交換で、外部組織から通知を受けたことがありますか



8. どこからの通知だったか、差し支えなければ教えてください

a. 著作権団体	2
b. 著作権者自身	1
c. その他:匿名者	1
c. その他:著作権者の権利が侵害されていないか監視する会社	1

9. 通知に、どのように対処しましたか

a. 利用者を特定し、対処した	4
b. 組織のネットワーク全体で該当する P2P 通信を禁止・制限した	1
c. 特に対処はしなかった	0
d. その他:利用者の特定や技術的な補助を行ったが、具体的な対処は P2P 通信を利用していた者の属する組織でしていただいた	1

10. その他 P2P に関するコメント等ありましたら、ぜひご記入ください

- 同様機能のソフトウェアが多数あり、また用途も多様でどれを規制すべきか理由が難しい。(B)
- P2P 技術を利用するアプリケーションが増えてきているが、これらの取り扱いについて組織内で規則ができていないため、個別に対応している状態ですっきりしていない。(C)
- Skype は制限していない。(C)
- 著作権侵害などが発生した場合、センターの所掌範囲をこえる。(C)
- 学術目的に限れば P2P も解放すべきだが、それ以外のものとの確証は得にくい。現時点では、BitTorrent 等を個別に解放している。(D)

- Winny WinMX Gnutella 等いくつかの著名なアプリケーションについては、検出サービスを買っている。また、BitTorrent は制限をしていなかったが、BitTorrent による著作権侵害に関する警告が来るようになったため、IDS で検知し警告するようにした。（E）
- Winny WinMX 等はキャッシュにより知らずに著作権侵害の片棒を担ぐ事があることと、情報漏洩事故の原因になりがちであるため禁止している。BitTorrent はダウンロードしているファイルを同時に他の利用者に公開もするため、違法ファイルを落とさなければ問題ないが、現実問題としてそういう利用者がいて問題となったため、特段の必要がない限り控えてもらうようにした。（E）
- 上記が禁止・制限の理由であるため、Skype や Groove のような不特定ファイル交換に関係のないアプリケーションについては制限していない。（E）
- 対応マニュアルを作成必要がある。（F）
- 著作権団体などが意図的にソーシャル攻撃をしている可能性がある。（F）
- Windows Vista に同包されている Live Messenger への対応に苦慮している。（G）

以上