

# 緊急情報セキュリティ アンケートへのご協力をお願い

皆様方には益々ご健勝のこととお慶び申し上げます。

Winny を始めとする P2P ソフトウェアに対するウイルスプログラムの蔓延は、個人情報、国家機密情報を始めとする重要情報の漏えいが大きな問題になっております。

そこで、緊急の情報セキュリティ調査を実施することに致しました。

2 枚目以降に質問がありますので、回答用紙にご記入・ご返送頂ければ幸いです。

あるいは、Excel ファイルを以下の URL からダウンロードし、印刷・送付することでも対応可能です (URL : <http://www2.gol.com/users/uchidak/research/>)

なお、質問は 2005 年 7 月 1 日から 2006 年 6 月 30 日を直近の 1 年とし、従業員数などは、6 月 30 日現在、あるいは、直近の決算日のものでご回答下さい。

本調査は情報セキュリティ管理者 (責任者・担当者) あるいは、情報システム管理者の方にご記入して頂きたいと考えております。

回答は、返信封筒にて回答用紙 (このページの裏、あるいは Excel にて作成・印刷したもの) のみ、ご返送頂くか、Excel ファイルを電子メールに添付してご返送下さい。なお、電子メールでの送付の場合、ファイルを暗号化しない場合には、セキュリティ上、100%安全でないことをご了解の上、ご送付下さい

なお、暗号化に必要な PGP の公開鍵はウェブ (<http://www2.gol.com/users/uchidak/>) にて公開しております。

また、大変お忙しいとは存じますが、アンケートは 2006 年 8 月末日 (木) までに、ご返送頂ければ幸いです。

ご質問・お問合せ先

内田 勝也 (うちだ かつや)

情報セキュリティ大学院大学 内田研究室 電話/FAX: 045-410-0238

電子メール: [uchidak@gol.com](mailto:uchidak@gol.com) または、[uchida@iisec.ac.jp](mailto:uchida@iisec.ac.jp) 携帯: 090-1050-3206

Web: <http://www2.gol.com/users/uchidak/> (左記 Web に PGP 公開鍵があります)

研究室に在室している事が少ないため、お手数ですが連絡は電子メール / FAX / 携帯電話にご連絡頂ければ幸いです (電子メールは大体毎日見えております)。

下記の回答で、【 】(1~6)等の場合には、1から6までの数字を、【 】内にご記入ください。  
下記の回答で、【 1 2 3 4 5 】等の場合には、該当する数字に全て をつけて下さい。

1. 回答者・回答企業の属性

- (1) 役職/所属部署【 】(1~8) (2) 主要業種【 】(1~19)  
(3) 従業員数【 】(1~11) (4) 電子商取引【 】(1~5)

2. セキュリティ関連事件履歴

- (5) ウイルス感染【 】(1~4) (6) 不正侵入【 】(1~4)  
(7) その他(原因: \_\_\_\_\_)【 】(1~4)  
(8.1) 人的ミス【 】(1~3) (8.2) ウィン-関連【 】(1~3)  
(8.1) その他【 】(1~3)

3. ウイルス対策現状 - 技術関連

- (9.1) クライアントPC【 】(1~9) (9.2) ファイルサーバ【 】(1~9)  
(9.3) インターネット【 】(1~9) (9.4) ストレージ【 】(1~9)  
(9.5) メールサーバ【 】(1~9) (9.6) ウェブサーバ【 】(1~9)  
(9.7) グループウェア【 】(1~9)  
(9.8) 集中管理ツール【 】(1~3) (9.9) 監視サービス【 】(1~3)  
(10.1) クライアントPC【 】(1~8) (10.2) ファイルサーバ【 】(1~8)  
(10.3) インターネット【 】(1~8) (10.4) ストレージ【 】(1~8)  
(10.5) メールサーバ【 】(1~8) (10.6) ウェブサーバ【 】(1~8)  
(10.7) グループウェア【 】(1~8)  
(11.1) ネットワーク監視【 】(1~3) (11.2) ウイルス監視【 】(1~3)  
(11.3) ファイアウォール監視【 】(1~3) (11.4) IDS/IPS 監視【 】(1~3)  
(11.5) その他監視( \_\_\_\_\_)【 】(1~3)  
(12) 収集情報利用【 】(1~4) (13) ネットワークの分離【 】(1~4)

4. ウイルス対策現状 - 組織関連

- (14) セキュリティ担当部署【 】(1~3) (15) 連絡・警告ルート【 】(1~3)  
(16) SP 遵守割合【 】(1~4)

5. 情報セキュリティ教育

- (17) 教育実施状況【 】(1~8) (18) 教育実施頻度【 】(1~4)  
(19) 実施テーマ【 1 2 3 4 5 6 7 8】(8: \_\_\_\_\_)  
(20) 今後の教育【 】(1~8)

6. ウイルス対策とセキュリティポリシー

- (21) 対策検討方法【 】(1~3)【3: \_\_\_\_\_】  
(22) 効果測定基準【 】(1~4)

7. ウイルス予防・リスク対策プロセス

- (23) 可用性向上対策【 】(1~4) (24) 脆弱性の把握程度【 】(1~4)  
(25) 定義ファイル【 】(1~5) (26) 配信方法【 】(1~4)  
(27) アカウント作成/削除【 】(1~4) (28) パスワード管理規則【 】(1~4)  
(29) バックアップ【 】(1~4) (30) ウィルス対応プロセス【 】(1~4)

8. 対応・復旧手順

- (31) 障害の一括管理【 】(1~4) (32) インシデント連絡方法【 】(1~4)  
(33) 発生原因究明【 】(1~5) (34) 情報入手先【 】(1~6)

**質問票** この票は送らないで下さい

1. 回答者・回答企業の属性
- (1) 役職/所属部署 (1つ選択)
- |                        |                          |
|------------------------|--------------------------|
| 1 経営/役員クラス             | 2 経営・経営企画部門 (社長室、経営企画室等) |
| 3 管理部門 (スタッフ部門・経理・総務等) | 4 情報システム部門の責任者           |
| 5 情報システム部門の担当者         | 6 その他の部門の責任者             |
| 7 その他の部門の担当者           | 8 その他                    |
- (2) 該当する主要業種 (1つ選択)
- |                      |                              |                      |
|----------------------|------------------------------|----------------------|
| 1 農林漁業・鉱業            | 2 建設業                        | 3 電気機械器具製造業 (情報通信電機) |
| 4 輸送用機械器具製造業 (自動車など) | 5 機械製造・材料系製造業 (その他機械、化学、金属等) | 6 その他製造業 (食品、繊維、出版等) |
| 7 電気・ガス・熱供給・水道業      | 8 運輸業                        | 9 通信業 (郵便・電気通信)      |
| 10 卸売業               | 11 小売業・飲食店                   | 12 金融業               |
| 13 情報サービス・調査・広告業     | 14 その他のサービス業                 | 15 医療機関・福祉・保健        |
| 16 不動産業              | 17 教育・学習支援 (小～大学、各種学校等)      | 18 公務 (政府・自治体)       |
| 19 その他               |                              |                      |
- (3) 従業員数 (1つ選択)
- |                  |                     |                |                |
|------------------|---------------------|----------------|----------------|
| 1 9人以下           | 2 10～49人            | 3 50～99人       | 4 100～299人     |
| 5 300～999人       | 6 1,000～2,999人      | 7 3,000～4,999人 | 8 5,000～9,999人 |
| 9 10,000～99,999人 | 10 100,000～149,999人 | 11 150,000人以上  |                |
- (4) 貴社の電子商取引について (1つ選択)
- |                        |                |              |
|------------------------|----------------|--------------|
| 1 自社運営 (自社サイト & 自社サーバ) | 2 サーバはハウジング    | 3 サーバはホスティング |
| 4 外部の電子商取引を利用          | 5 電子商取引を行っていない |              |
2. セキュリティ関連事件履歴 (各項目で1つ選択)
- 過去3年間を考えた場合、
- |  |    |      |      |      |
|--|----|------|------|------|
|  | ない | 1～2回 | 3～4回 | 5回以上 |
|--|----|------|------|------|
- (5) 年間平均のウイルス大規模感染回数
- |  |   |   |   |   |
|--|---|---|---|---|
|  | 1 | 2 | 3 | 4 |
|--|---|---|---|---|
- (6) 年間平均の不正侵入回数
- |  |   |   |   |   |
|--|---|---|---|---|
|  | 1 | 2 | 3 | 4 |
|--|---|---|---|---|
- (7) その他の原因 ( ) による年平均の事件発生件数
- |  |   |   |   |   |
|--|---|---|---|---|
|  | 1 | 2 | 3 | 4 |
|--|---|---|---|---|
- (8) 情報漏えい事件
- |                     |       |       |       |
|---------------------|-------|-------|-------|
| 8.1 人的ミス            | 1. あり | 2. なし | 3. 不明 |
| 8.2 ウイニー/Share 等に関連 | 1. あり | 2. なし | 3. 不明 |
| 8.3 その他             | 1. あり | 2. なし | 3. 不明 |
3. ウイルス対策現状 - 技術関連 (各項目で1つ選択)
- (9) ウイルス対策製品の導入状況について
- |                   |   |   |   |   |   |   |   |   |   |
|-------------------|---|---|---|---|---|---|---|---|---|
| 9.1 クライアントPC      | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 |
| 9.2 ファイルサーバ       | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 |
| 9.3 インターネットゲットウェイ | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 |
| 9.4 ストレージ         | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 |
| 9.5 メールサーバ        | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 |
| 9.6 ウェブサーバ        | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 |
| 9.7 グループウェア       | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 |
- 注) 回答の1～9は以下のようになっています。
- |           |           |           |           |           |
|-----------|-----------|-----------|-----------|-----------|
| 1. 50%未満  | 2. 50～59% | 3. 60～69% | 4. 70～79% | 5. 80～89% |
| 6. 90～99% | 7. 100%   | 8. 不明     | 9. 未導入    |           |
- 9.8 ウイルス対策集中管理ツールの導入
- |       |        |       |
|-------|--------|-------|
| 1. 導入 | 2. 未導入 | 3. 不明 |
|-------|--------|-------|
- 9.9 ウイルス監視サービスの利用
- |       |        |       |
|-------|--------|-------|
| 1. 利用 | 2. 未利用 | 3. 不明 |
|-------|--------|-------|
- (10) ウイルス定義 ファイルの更新目標値について (各項目で1つ選択)
- |                    |   |   |   |   |   |   |   |   |
|--------------------|---|---|---|---|---|---|---|---|
| 10.1 クライアントPC      | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 |
| 10.2 ファイルサーバ       | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 |
| 10.3 インターネットゲットウェイ | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 |

**質問票** この票は送らないで下さい

|      |            |   |   |   |   |   |   |   |   |
|------|------------|---|---|---|---|---|---|---|---|
| 10.4 | ストレージ      | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 |
| 10.5 | メールサーバ     | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 |
| 10.6 | ウェブサーバ     | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 |
| 10.7 | グループウェアサーバ | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 |

注) 回答の1～9は以下のようになっています。

1. 30分未満    2. 30～59分    3. 60～89分    4. 90～119分    5. 120分以上  
6. 目標値未設定    7. 不明    8. 未導入

定義ファイル：ウイルス等の特徴を収録したファイル。最新の対策のために随時アップデートが必要

(11) ネットワーク等の監視状況について (各項目で1つ選択)

|      |             |   |   |   |
|------|-------------|---|---|---|
| 11.1 | ネットワーク監視    | 1 | 2 | 3 |
| 11.2 | ウイルス感染監視    | 1 | 2 | 3 |
| 11.3 | ファイアウォール監視  | 1 | 2 | 3 |
| 11.4 | IDS / IPS監視 | 1 | 2 | 3 |
| 11.5 | その他監視 ( )   | 1 | 2 | 3 |

- |   |                             |
|---|-----------------------------|
| 1 | 十分な監視をしており、自社への侵入の大部分を検出できる |
| 2 | 監視をしているが、自社への侵入を常に検出できてはいない |
| 3 | 監視/検出機能は使用していない             |

(12) 監視システムによる収集情報の利用 (1つ選択)

- 1 情報は収集・分析後、監視システムでいくつかのレポートへ自動変換される
- 2 情報は収集・分析後、手作業により、いくつかのレポートにまとめられる
- 3 情報は生データのログ形式で収集・保管され、分析はほとんど/まったく行われていない
- 4 未導入

(13) 基幹システムと他の情報系システムでのネットワークセグメントの分離 (1つ選択)

- 1 分離されており、ネットワーク間の接続は許可されていない
- 2 分離されているが、ネットワーク間でごく一部の接続が許可されている
- 3 分離されていない
- 4 不明

4. ウイルス対策現状 - 組織関連

(14) セキュリティ担当部署について (1つ選択)

- 1 役割と責任が明確に規定された専任部門があり、問題発生時の対応フローが明確化されている
- 2 特定の組織はないが、役割と責任が規定されている専任者がセキュリティ問題を担当
- 3 専任の部署・担当者はいない

(15) 最新のセキュリティ脅威をユーザに連絡・警告ルートについて (1つ選択)

- 1 ユーザへの連絡・警告ルートがある (ニュースレターやメール等)
- 2 ルートはあるが、深刻な脅威に対してのみ使用
- 3 ルートは特になし。連絡・警告はその時々で行われる

(16) セキュリティポリシー (Web 閲覧規則、添付ファイル開封規則等) 遵守割合 (1つ選択)

- 1 50%未満    2 50～80%    3 81%以上    4 不明

5. 情報セキュリティ教育について

(17) 従業員向け情報セキュリティ教育の実施状況について (1つ選択)

- 1 大学院等長期の教育機関へ派遣している
- 2 社内で体系的な教育 (数ヶ月程度) を実施している
- 3 外部の体系的な教育 (1週間程度) へ参加させている
- 4 外部の1～数日のセミナー (有償) へ参加させている
- 5 外部の1～数日のセミナー (無償) へ参加させている
- 6 OJT、自習のみ
- 7 不要と考えている
- 8 不明

(18) 従業員向けセキュリティ教育の実施頻度について

- 1 年1～2回    2 年3～4回    3 年5回以上    4 まったく/ほとんど実施していない。

(19) セキュリティ教育テーマ (該当するもの全てを選択)

**質問票** この票は送らないで下さい

- 1 ウイルス
  - 2 その他のセキュリティの脅威 (フィッシング、スパイウェア等)
  - 3 ソーシャルエンジニアリング
  - 4 セキュリティポリシー
  - 5 セキュリティマネジメント
  - 6 暗号関連
  - 7 パスワード等の個人認証
  - 8 その他 (具体的に: )
- (20) 今後の情報セキュリティ教育について (1つ選択)
- 1 大学院等長期の教育機関へ派遣したい
  - 2 社内で体系的な教育 (数ヶ月程度) の実施
  - 3 外部の体系的な教育 (1週間程度) へ参加させる
  - 4 外部の1~数日のセミナー (有償) へ参加させる
  - 5 外部の1~数日のセミナー (無償) へ参加させる
  - 6 OJT、自習のみ
  - 7 不要と考えている
  - 8 不明
6. ウイルス対策とセキュリティポリシー
- (21) セキュリティ対策の検討方法はどれに該当しますか (1つ選択)
- 1 リスクアセスメント段階からユーザー部門が参画し、業務影響度に基づいて投資 (費用) 対効果を考慮して対策の立案が行われる
  - 2 セキュリティ対策は全て IT 部門で検討
  - 3 その他 (具体的に: \_\_\_\_\_)
- (22) ウイルス対策管理の効果測定基準が組織内にありますか (1つ選択)
- 1 全体のセキュリティ効果に加え、ウイルス対策効果も数値目標を用いて別途測定
  - 2 セキュリティ効果はある程度測定しているが、ウイルス対策効果は特に測定していない
  - 3 セキュリティ効果はいつさい測定されません
  - 4 不明
7. ウイルス予防・リスク対策プロセス
- (23) ウイルス対策ソフトの定義ファイル安定供給の仕組みやマルチレイヤーによるウイルス対策など、可用性向上の仕組み (1つ選択)
- 1 業務影響度と投資 (費用) 対効果の両方を考慮した可用性向上のシステムが構築・運用されている
  - 2 製品の仕様上可能な限りの可用性向上を実現している
  - 3 可用性を向上させるための仕組みは特にない
  - 4 不明
- (24) 現行システムの脆弱性の把握程度について (1つ選択)
- 1 脆弱性レベルは常に把握されており、また常時監視を行っている
  - 2 不定期に脆弱性検査を行い、脆弱性レベルをチェックするが、検査範囲は十分でない
  - 3 ほとんど把握できていない
  - 4 不明
- (25) ウイルス対策ソフトのエンジン・定義ファイルの番号管理の実施 (1つ選択)
- 1 100% 管理されている
  - 2 ほぼ管理されているが、確認のためのプロセスはない
  - 3 あまり管理されていない
  - 4 まったく管理されていない
  - 5 不明
- (26) セキュリティパッチ・検索エンジン・定義ファイル・駆除ツール等の配信方法 (1つ選択)
- 1 必要に応じて自動配信される
  - 2 IT スタッフが配信と監視を行い、十分な配信レベルを確保
  - 3 各エンドユーザーが手動でアップデートを行い、特に追跡機能はない
  - 4 不明
- (27) ネットワークアカウント作成/削除時のユーザー部門によるチェック (1つ選択)
- 1 アカウント作成時に人事部及びユーザー部門長が確認し、「未利用アカウント」が発生しないよう無効アカウントを定期的に削除している
  - 2 ユーザー部門による確認だけで、そのアカウントが「未利用アカウント」かを知る方法はない
  - 3 ユーザー部門による確認作業は実施していない
  - 4 不明
- (28) パスワード管理規則 (形式、アップデート頻度、暗号化など) について (1つ選択)
- 1 パスワード管理規則があり、全員が事前に定義された形式・更新頻度を遵守している
  - 2 パスワード管理規則はあるが、遵守されているかは管理されていない

質問票 この票は送らないで下さい

- 3 パスワード管理規則はない                      4 不明
- (29) システムバックアップの仕組みはありますか (1つ選択)
- 1 アプリケーションサーバとウイルス対策サーバに対するシステムバックアップの仕組みはある  
2 システムバックアップの仕組みがあが、対象は最重要サーバだけで、ウイルス対策サーバは対象外  
3 仕組みはない    4 不明
- (30) 組織内にウイルス大規模感染への対応プロセスはありますか? (1つ選択)
- 1 対応プロセスがあり、大規模感染時には常に遵守される  
2 対応プロセスはあるが、遵守されないことがある  
3 対応プロセスがないため、ケースバイケースで対応    4 不明
8. 対応・復旧手順
- (31) セキュリティインシデントは、他のシステム障害と一括管理されていますか? (1つ選択)
- 1 すべて一括管理    2 セキュリティインシデントは他の障害とは別に管理  
3 セキュリティインシデントは特に管理されていない    4 不明
- (32) インシデントに対し、社内間・社外ベンダーへの連絡方法は明確に定義されていますか? (1つ選択)
- 1 社内間、社外両方とも連絡方法は明確に定義されている  
2 社内間 (ユーザ サービスデスク 担当者) は明確に定義されている  
3 明確に定義されていない    4 不明
- (33) インシデントの発生原因の究明 (1つ選択)
- 1 常に原因究明され、再発防止策も検討している  
2 原因究明がされているが、再発防止策の検討はない  
3 原因究明は定常的に実施されていない    4 原因究明は全く実施されていない  
5 不明
- (34) インシデントの原因究明・再発防止策の検討で、情報の入手先 (1つ選択)
- 1 ウイルス対策ベンダーの Web  
2 ウイルス対策ベンダーのサポートセンター  
3 購入店・Sier からの情報    4 雑誌・書籍・インターネットなどの一般情報  
5 その他    6 不明

ありがとうございました。アンケートは以上です。同封の返信封筒にて、回答用紙のみご返送下さい。  
アンケートは全て統計的な処理を行い、全ての内容について貴組織名、ご記入者名等の個別属性を公開することはありません。また、ご記入頂いた内容は、本アンケートに関連するもの以外には利用いたしません。

ご質問・お問合せ先

内田 勝也 (うちだ かつや)

情報セキュリティ大学院大学 内田研究室 電話/FAX: 045-410-0238

電子メール: uchidak@gol.com または、 uchida@iisec.ac.jp 携帯: 090-1050-3206

Web: <http://www2.gol.com/users/uchidak/> (左記 Web に PGP 公開鍵があります)

研究室に在室している事が少ないため、お手数ですが連絡は電子メール / FAX / 携帯電話にご連絡頂ければ幸いです (電子メールは大体毎日見ております)。