第４回情報セキュリティ アンケートへのご協力のお願い

皆様方には益々ご健勝のこととお慶び申し上げます。

情報システムは今や企業・組織だけでなく、一般社会における重要な基盤であると言えます。 それに伴い、情報システムの安全性・信頼性を確保するための情報セキュリティ対策が非常に重要になってきました。

中央大学 ２１世紀ＣＯＥ研究の一環として、首記アンケートを実施しております。 このアンケートは、米国 CSI（Computer Security Institute）が、FBI と協力して過去 10 数年間、情報セキュリティ調査を行っていますが、それに準拠したアンケートを実施し、日米の情報セキュリティ比較を試みるものです。

今回は第４回目の調査で、今後も毎年実施したいと考えております。 皆様方のご協力をお願いいたします。

次ページ以降に質問がありますので、回答用紙にご記入頂き、返送頂くか、Excel ファイルを以下の URL からダウンロードし、印刷・送付できます（URL：http://www2.gol.com/users/uchidak/research/ ）。

なお、**質問は 2006 年 1 月 1 日から 2006 年 12 月 31 日を対象期間**とし、従業員数、PC 台数、総所得金額などは、12 月 31 日現在、あるいは、直近の決算日のものでご回答下さい。

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利用することはありません。

本調査は情報セキュリティ管理者（CISO、CISO 補佐等）の方々あるいは情報システム担当の方々などにご記入して頂きたいと考えております。

回答は、同封の**返信封筒にて回答用紙（同封のもの、あるいは Excel にて作成・印刷したもの）のみを返送**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、**PGP の公開鍵はウェブに公開しております**）。

また、大変お忙しいとは存じますが、**アンケートは2007年1月末日（火）まで**に、ご返送頂ければ幸いです。

なお、昨年度までの集計結果ならびに、「CSI/FBI Computer Crime & Security Survey」の日本語解説は、下記ウェブに保存してありますので、ご自由にご利用下さい。

ご質問・お問合せ先　　uchidak　**検索**　Google で検索できます

内田　勝也
〒112-8551 東京都文京区春日 １－13－27
中央大学 研究開発機構 情報システム人材育成ユニット
研究室 電話: 03-3817-1631 FAX: 03-3817-1606 携帯: 090-1050-3206
あるいは、
情報セキュリティ大学院大学 研究室 電話/FAX: 045-410-0238
電子メール: uchidak@gol.com　Web: http://www2.gol.com/users/uchidak/
（PGP 公開鍵は上記 URL にあります）
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あるいは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）。

質 問 票　この票は送らないで下さい

1．貴組織・ご記入者について　（不明な項目は 未記入で構いません）

1-1. 従業員数（１つを選択）

1：1 ～ 99 人	2：100 ～ 299 人	3：300 ～ 499 人	4：500 ～ 999 人
5：1,000 ～ 1,499 人	6：1,500 ～ 9,999 人	7：10,000～49,999 人	8：50,000 人以上

1-2. 総所得金額（１つを選択）

1：１億円未満	2：1 ～ 9 億円	3：10 ～ 99 億円
4：100 ～ 499 億円	5：500 ～ 999 億円	6：1,000 億円以上

1-3 該当する主要業種（１つを選択）

1．建設業	2．電気･ガス･水道業	3．運輸業	4．金融･保険業
5．製造業	6．情報通信業	7．ハイテク	8．卸売･小売業
9．不動産業	10．飲食店･宿泊業	11．医療･福祉	12．教育･学習支援
13．複合サービス業	14．法務・法律	15．公務(政府･自治体)	16．その他

1-4 ご記入者の所属（１つを選択）

1．総務	2．人事	3．経理
4．社長室	5．企画部門	6．情報システム管理部門
7．情報システム開発部門	8．事業部門	9．その他

1-5 ご記入者の役職（１つを選択）

1．会長・社長・役員	2．執行役員	3．事業部長
4．部長	5．課長	6．係長・主任
7．専門職	8．一般社員	9．その他

1-6 該当する役職（１つを選択）

1．ＣＥＯ	2．ＣＩＯ	3．ＣＳＯ	4．ＣＩＳＯ
5．セキュリティ部門管理職	6．システム管理者	7．その他	

2．貴組織のシステムについて

2-1. パソコンの台数（１つを選択）

1．10 台未満	2．11 ～ 99 台	3．100 ～ 999 台	4．1,000 台以上

2-2. インターネットへの主たる接続方法（１つ選択）

1．未接続	2．ﾀﾞｲｱﾙｱｯﾌﾟ	3．常時接続（ADSL/CATV/光ｹｰﾌﾞﾙ等）	4．常時接続（専用線）

2-3. 電子商取引(**EC**)や個人情報(**PI**)の収集をウェブで行っていますか？

1．EC のみ	2．PI のみ	3．EC&PI とも	4．行っていない

3．情報セキュリティ予算・教育等

3-1 情報セキュリティ予算額は（１つ選択）

1．～499 万	2．500～999 万	3．1,000～5,000 万	4．5,000～1 億	5．１億以上	6．不明

3-2 情報セキュリティ予算が情報システム予算に占める割合は（１つ選択）

1．1%未満	2．1～2%	3．3～5%	4．6～7%	5．8～10%	6．10%以上	7．不明

3-3 情報セキュリティの投資効果を計算している場合、その方法（１つ選択）

1．ROI	2．NPV	3．IRR	4．その他	5．不明	6．計算していない

3-4 情報セキュリティ保険に加入していますか？（１つ選択）

1．加入している	2．加入していない

3-5 情報セキュリティ監査を実施していますか？（１つ選択）

1．内部監査のみ実施	2．外部監査のみ実施	3．内部･外部とも実施	4．実施していない

3-6 情報セキュリティの外注割合（１つ選択）

1．なし	2．1～20%	3．21～40%	4．41～60%	5．61～80%	6．81%～100%

3-7 情報セキュリティ教育の実施レベル（0:何もしていない･･･7. 相当程度実施している）（１つ選択）

0．ない	1．最低	2．	3．	4．	5．	6．	7．最高

質 問 票　この票は送らないで下さい

3-8 情報セキュリティ教育で重要だと思われるものご回答下さい（いくつでも）

1．セキュリティポリシー	2．ネットワークセキュリティ	3．アクセス制御システム
4．セキュリティマネジメント	5．セキュリティの経済側面	6．セキュリティシステム構成
7．情報法科学(Information Forensics)	8．暗号関連	9．セキュリティ投資／法律

4．貴組織にて情報セキュリティ利用技術（ご利用のものをいくつでも）

1．ファイアウォール	2．ワクチンソフト（アンチウィルスソフト）	3．アンチ・スパイウェア
4．アクセス制御（サーバ用）	5．侵入検知システム：IDS	6．送信中のデータ暗号化
7．保存ファイルの暗号化	8．一般的なパスワード	9．侵入防止システム：IPS
10．ログ管理ソフトウェア	11．アプリケーションファイアウォール	12．IC カード
13．ワンタイムパスワード	14．フォレンジックスソフト	15．ＰＫＩ
16．無線 LAN セキュリティソフト	17．バイオメトリックス	18．その他

5．過去１年間に無権限者によるコンピュータ利用（１つ選択）

1．利用された	2．利用されたことはない	3．わからない

6．セキュリティ事故（インシデント）として以下のものが発生したことがありますか？（該当するものがあれば、いくつでも）

1. ウイルス感染	2. 情報への不正アクセス	3. ノート PC などの盗難
4. 情報資産の盗難	5. DoS攻撃	6. 金融詐欺
7. 内部者のネット・アクセス乱用(1)	8. 通信詐欺(2)	9. システムがボットネットに悪用された
10. システム侵入	11. システムが Phishing に悪用された	12. 無線 LAN の無許可利用
13. IM（インスタントメッセージ）の悪用	14. ファイル破壊／改ざん	15. ウェブの改ざん
16. パスワード盗聴	17. DNS サーバが悪用された	18. その他
19. 発生していない		

注 1）ポルノ画像のダウンロード、プログラム等の違法コピー、私用メール利用等、セキュリティポリシー違反に対する処罰
注 2）通信詐欺：①通信サービスを提供したようみせ、その費用を他人からだまし取る。②通信サービスの費用を他人のクレジットカード、電話等に請求させてしまう、等の犯罪

7．セキュリティ事故（インシデント）の発生回数（過去１年間）

	外部犯行	内部犯行		外部犯行	内部犯行
1～ 5 回	11	21	31 回以上	14	24
6～10 回	12	22	不 明	15	25
11～30 回	13	23	発生ゼロ	16	26

8．ウェブサイトのセキュリティ事故（インシデント）

8-1 セキュリティ事故（無権限アクセス、改竄、情報漏洩）の発生回数（どれか１つ）

1．ない	2．１～５回	3．６～10 回	4．10 回以上

8-2 上記 8-1 でセキュリティ事故の発生は 内部／外部からですか？（１つ選択）

1．内部	2．外部	3．両方	4．不明

8-3 上記 8-1 で発生したセキュリティ事故は下記のどれが発生しましたか？（いくつでも）

1．ウェブの改竄	2．金融詐欺	3．サービス妨害（DoS 攻撃）	4．情報の窃盗
5．その他			

9．外部からの攻撃について

9-1 攻撃を受けた場所（いくつでも）

1．内部システム	2．ダイアルアップ回線	3．インターネット
4．無線ＬＡＮ	5．その他	6．ない

9-2 攻撃相手は誰だと思われますか（いくつでも）

1．ハッカー／クラッカー（国内）	2．ハッカー／クラッカー（海外）	3．競合他社（国内）
4．競合他社（海外）	5．海外の国家・政府	6．従業員
7．不 明		

質 問 票　この票は送らないで下さい

10. セキュリティ事故（インシデント）による費用（該当するものすべて）

セキュリティ事故は質問６と同じです

セキュリティ事故	直接的費用（単位 円）	間接的費用（単位 円）
1. ウイルス感染		
2. 情報への不正アクセス		
3. ノート PC などの盗難		
4. 情報資産の盗難		
5. DoS攻撃		
6. 金融詐欺		
7. 内部者のネット・アクセス乱用(注1)		
8. 通信詐欺(注2)		
9. システムがボットネットに悪用された		
10. システム侵入		
11. システムが Phishing に悪用された		
12. 無線 LAN の無許可利用		
13. IM（インスタントメッセージ）の悪用		
14. ファイル破壊／改ざん		
15. ウェブの改ざん		
16. パスワード盗聴		
17. DNS サーバが悪用された		
18. その他		
19. 発生していない		

- 直接的費用：①被害システムの復旧を行った従業員の人件費、②復旧を外部委託した場合の費用、③再発防止に必要なソフトウェア等の購入費用等。　例：人件費の計算：50,000 円／人日（6,000 円／人時）
- 間接的費用：①被害により利用者がパソコンを利用できないための機会損失、②情報漏洩によるお詫び広告費用、③訴訟のための弁護士費用等　例：パソコンが利用できなかった利用者の機会損失：人件費の 20%程度（10,000 円／人時）

11. ネットワークへの侵入を経験した方に。以下のどれを行いましたか？（いくつでも）

1．セキュリティのパッチを実行した	2．担当部門だけで処理した
3．外部へ報告しなかった	4．経営トップには報告した
5．弁護士に相談した	6．IPA/JPCERT 等に届け出た
7．警察へ届け出た	8．何もしなかった

12. 警察/IPA に届けなかった理由は？（いくつでも）

1．外部からマイナスイメージを持たれる恐れがあったため
2．競合他社に利用される恐れがあったため
3．報告をしようという考えに至らなかった
4．社内対応で十分だと判断した
5．その他

13. 外部のセキュリティ組織に所属していますか？（いくつでも）

1．日本セキュリティ・マネジメント学会	2．情報処理学会
3．電子情報通信学会	4．日本ネットワークセキュリティ協会 JNSA
5．日本セキュリティ監査協会 JASA	6．インターネット協会
7．情報ネットワーク法学会	8．ネットワークリスクマネジメント協会 NRA
9．Telecom-ISAC	10．その他　　11．どこにも所属していない

14. 情報セキュリティ確保のため、最も効果的なものはどれですか？（いくつでも）

1. 内部セキュリティ監査	2. ペネトレーションテスト	3. 脆弱性検査ソフト	4. 外部セキュリティ監査
5. メール監視ソフト	6. ウェブ監視ソフト	7. その他	8. なし

ありがとうございました。以上でアンケートは修了です。同封の返信封筒にて、**回答用紙のみ**ご返送下さい。