2013 年度 情報セキュリティ事象被害状況調査票

独立行政法人 情報処理推進機構

◎ 貴社の「情報セキュリティに関する管理者（責任者・担当者）の方」がご回答ください。
貴方がそれ以外の方の場合は、お手数ですが、該当される者にお渡しくださいますようお願いいたします。

◎ 情報処理推進機構セキュリティセンターでは、国内の企業における「情報セキュリティに関する被害状況を捉える」ことを目的としたアンケートを実施しております。今回の調査結果は、2014 年 1 月頃、情報処理推進機構セキュリティセンターのホームページにて公開する予定です。ご回答の内容については、すべて統計数値として集計いたしますので、会社名や個人名、個別のご回答内容などが公表されることは一切ございません。

◎ 本調査の設問数は、33問（セキュリティ事象を経験していない企業）～最大48問（セキュリティ事象を経験した企業）です。セキュリティ事象被害の実態を広く捉え、統計的に有意な結果を得るために、ご回答へのご協力を何卒よろしくお願い申し上げます。

◎ この調査の実施、取り纏めにつきましては、みずほ情報総研株式会社に委託しております。

◎ 本調査へのご回答には、以下の3種類の方法がございます。いずれか1つの方法でご回答ください。

方法1） 本調査票にご記入いただき、郵送にてご返送いただく

・お答えは、特に説明のないかぎり、あてはまる項目をお選びのうえ、該当する番号に○をご記入ください。
また、お答えが「その他」にあてはまる場合は、（ ）にその内容を具体的にご記入ください。
・お答えいただいた内容により、次にご回答いただく設問が変わる場合ありますので、調査票上の説明にご注意ください。
・ご記入いただいた用紙は、同封の返信用封筒（切手不要）に入れ、平成 25 年 10 月 4 日（金）までにご投函くださいますようお願い申し上げます。

方法2） アンケート回答用ウェブページにてご回答いただく

・楽天リサーチ株式会社の提供するアンケートシステムを用いて回答結果の収集を行います。このとき、貴社名と回答 ID の対応関係を楽天リサーチ株式会社は関知せず、ご回答いただいた内容を同社が利用することもございません。
・次の手順でご回答ください。（平成 25 年 10 月 4 日（金）まで）
① 本調査票に同封した「ご協力のお願い」に記載された回答 ID とパスワードをご用意ください。（貴社専用の ID です）
② ウェブブラウザにて、「ご協力のお願い」に記載された URL にアクセスしてください。
③ ①で用意した ID とパスワードでログインし、表示される設問にご回答ください。

方法3） 電子媒体の調査票をダウンロードして回答し、電子メールにてご返送いただく

・次の手順でご回答ください。（平成 25 年 10 月 4 日（金）まで）
① 下記 URL から電子媒体の調査票ファイル（Microsoft Excel 形式）をダウンロードします。
（URL： http://www.ipa.go.jp/security/）
② ダウンロードした調査票ファイルにて、回答を選択もしくは記入してください。
③ ②のファイルに必要に応じてパスワード（Microsoft Excel のパスワード、ZIP パスワード、貴社規定の方式のいずれでも可）を付与してください。パスワードについては、恐れ入りますが、お電話、FAX、電子メールのいずれかの手段で別途下記【調査実施に関するお問合せ先】までご連絡をお願いいたします。
④ ご回答いただいたファイルを電子メールに添付し、下記のアドレスまでご返送くださいますようお願い申し上げます。
返送先電子メールアドレス： sec-enq@mizuho-ir.co.jp

◎ 本調査についてご不明な点がございましたら、下記までお問合せください。

【調査主旨に関するお問合せ先】
独立行政法人情報処理推進機構
技術本部 セキュリティセンター
担当：花村、小松
電話：03-5978-7530
E-mail: isec-survey@ipa.go.jp

【調査実施に関するお問合せ先】
みずほ情報総研株式会社
経営・IT コンサルティング部
担当：小川、築島、冨田、能瀬
電話：03-5281-5492 FAX：03-5281-5429
E-mail: sec-enq@mizuho-ir.co.jp

この調査は、貴社全体の状況についてお答えください

Ⅰ. 貴社についてお伺いします。

問 1　貴社の主な業種をお答えください。（○は 1 つ）

1　食料品、飲料・たばこ・ 飼料製造業	2　繊維工業	3　パルプ・紙・紙加工品製造業
4　化学工業	5　石油・石炭・プラスチック製品 製造業	6　窯業・土石製品製造業
7　鉄鋼業	8　非鉄金属・金属製品製造業	9　電気機械器具製造業
10　情報通信機械器具製造業	11　輸送用機械器具製造業	12　その他機械器具製造業
13　その他の製造業	14　農林漁業・同協同組合、 鉱業	15　建設業
16　電気・ガス・熱供給・ 水道業	17　映像・音声情報制作・放送・ 通信業	18　新聞・出版業
19　情報サービス業	20　運輸業・郵便業	21　卸売業
22　小売業	23　金融業・保険業	24　医療業（国・公立を除く）
25　教育（国・公立を除く）、学習支援業	26　その他のサービス業	

問 2　貴社の総従業員数（有給役員,正社員・正職員,準社員・準職員,アルバイト等を含む）について、2012 年度（2012 年 4 月～2013 年 3 月）の人数をお答えください。

※常時従業者の総数。有給役員及び常時雇用者（正社員・正職員、準社員・準職員、アルバイト等、1 ヶ月を超える雇用契約者）とし、人材派遣業者からの派遣従業者は含めません。

人

問 3　貴社の総売上高（単体）について、2012 年度（2012 年 4 月～2013 年 3 月）の金額をお答えください。

※決算期が 3 月でない場合、決算期に合わせた回答で構いません。
※学校、組合団体など営業活動を行わない組織の場合は、当該年度における収入高とします。

兆	千億	百億	十億	億	千万	百万

百万円

問 4　貴社の経常利益（単体）について、2012 年度（2012 年 4 月～2013 年 3 月）の金額をお答えください。

※決算期が 3 月でない場合、決算期に合わせた回答で構いません。
※マイナスの場合は先頭に△をお付けください。

兆	千億	百億	十億	億	千万	百万

百万円

問 5　貴社の規定年間営業日数および1日の営業時間をお答えください。

a. 年間営業日数	日/年
b. 1 日あたり営業時間	時間/日

問 6　貴社は上場していますか。（○は 1 つ）

1　上場している　　2　上場していない

問 7　貴社に海外拠点はありますか。（○は 1 つ）

1　無し　　2　有り

問 8　貴社の IT 関連の支出総額について、2012 年度（2012 年 4 月～2013 年 3 月）の費用を、概算でわかる範囲でお答えください。（問 22 における情報セキュリティ関連の支出を含んだ支出額をご記入ください。）（○は1つ）

1　1 百万円未満　　2　1 百万円～5 百万円未満　　3　5 百万円～1 千万円未満
4　1 千万円～2 千万円未満　　5　2 千万円～5 千万円未満　　6　5 千万円～1 億円未満
7　1 億円～4 億円未満　　8　4 億円以上　　9　わからない

問 9　貴社で電子商取引（EC）業務[*1] を行っている場合、電子商取引（EC）業務の売上が、全体の売上に占める割合について、最も近いものをお答えください。電子商取引（EC）業務を行っていない場合は「0%」を選択して下さい。（○は 1 つ）

*傘下事業所（支社・支店・出張所等）も含めてお答えください。

1　0%　　2　10%　　3　20%
4　30%　　5　40%　　6　50%
7　60%　　8　70%　　9　80%
10　90%　　11 100%

（*1）　ここでは電子商取引（EC）業務を、「インターネット技術を用いたコンピュータ・ネットワーク・システムを介して受発注などの商取引が行われ、かつその成約金額が捕捉されるもの」と定義します。電話や FAX による受発注は含まず、電子メールによる受発注のうち定型フォーマットによらないものも含みません。支払についてはコンピュータ・ネットワーク・システムを介して行われるかどうかを問いません。

問 10 貴社では自組織内でサーバを設置・運用していますか（○は1つ）。設置・運用している場合は、わかる範囲でその台数（仮想的なものを含まない）をご記入ください。なお、クラウドコンピューティングサービスとして利用しているサーバは台数に加えないでください。

1　有り（約　　）台　　2　無し

→ 問 10-1　問 10 で自組織内でサーバを設置・運用していると回答された方にお尋ねします（以下、問 10-2 まで同じ）。貴社では、文書管理用サーバ、グループウェア用サーバ、プリントサーバ、DNS サーバ以外のサーバを保有していますか。（○は1つ）

1　有り　　2　無し

→ 問 10-2　貴社では、自社で設置しているサーバにおいて、ウェブアプリケーションを利用していますか。（○は1つ）

1　利用している　　2　利用していない

問 11 貴社で利用されているクライアント(パソコン)を保有していますか（○は1つ）。保有している場合は、台数をご記入ください。なお、シンクライアント端末を導入している場合は、その端末も含めてカウントしてください。

1　有り（約　　）台　　2　無し

問 12 貴社では、従業員等によるインターネットの利用（例：ウェブブラウザによるアクセス）が可能ですか。正規職員と非正規職員に分けてご回答ください。（○は1つ）

問 12-1　（正規雇用の従業員）

1　ほぼ全員利用できる　　2　概ね半数以上は利用可能
3　概ね半数未満が利用可能　　4　全員利用できない

問 12-2　（非正規雇用の従業員）

1　ほぼ全員利用できる　　2　概ね半数以上は利用可能
3　概ね半数未満が利用可能　　4　全員利用できない
5　非正規雇用の従業員はいない

問 13 貴社では、スマートフォンやタブレット端末を業務において利用していますか。（○は 1 つ）

1 利用している　　2 利用を検討中　　3 利用していない

→問 13-1 問 13 でスマートフォンやタブレット端末を業務において利用していると回答された方にお尋ねします（以下、問 13-5 まで同じ）。利用している端末は何ですか。（○はいくつでも）

1 スマートフォン（iOS）　　2 スマートフォン（Android 系）
3 スマートフォン（その他）　　4 タブレット端末（iOS）
5 タブレット端末（Android 系）　　6 タブレット端末（その他）

→問 13-2 利用端末（会社支給端末及び会社に登録済みの私有端末）台数と、そのうち会社支給の端末の比率をお答えください。

a. スマートフォン　約＿＿＿＿＿＿台　　b. タブレット端末　約＿＿＿＿＿＿台
→うち、会社支給の比率　約＿＿＿＿％　　→うち、会社支給の比率　約＿＿＿＿％

→問 13-3 利用用途は何ですか。（○はいくつでも）

1 通話、メール等の連絡　　2 スケジューラ
3 社内 SNS　　4 プレゼンテーション、資料提示
5 営業支援（顧客データ閲覧、入力）　　6 在庫管理
7 その他（　　）

→問 13-4 以下のうちスマートフォンやタブレット端末において実施している対策をお答えください。（○はいくつでも）

1 端末のパスワード設定　　2 紛失・盗難時のデータ消去
3 セキュリティソフトの導入　　4 MDM[*2] による端末管理
5 利用ルールの策定（アプリケーションの導入制限等）　　6 その他（　　）
7 特に実施していない

（*2） MDM（Mobile Device Management、モバイル端末管理）とは、モバイル端末と社内システムとの認証、アプリケーションとの同期、外部サービスとの接続等を管理するシステム

→問 13-5 スマートフォンやタブレット端末について、社員の私有端末の業務利用（BYOD: Bring Your Own Device）を認めていますか。（○は 1 つ）

1 認めている　　2 現在、認めるかどうかを検討中
3 今後、認めるかどうかの検討を予定している　　4 認める予定はない

問 14 クラウドコンピューティングで提供される下記のサービスのうち、貴社で利用している用途をすべて選択してください。（○はいくつでも）

1 電子メールやスケジューラ、各種コミュニケーションのための利用（パブリッククラウド＝他ユーザと機器設備を共用）	
2 業務アプリケーションの利用（パブリッククラウド）	3 ファイルサーバとしての利用（パブリッククラウド）
4 プライベートクラウド（他ユーザとの共用無し）としての利用	5 1～4 以外の方法による利用

6 クラウドコンピューティングサービスは利用していない

→問 14-1 問 14 でクラウドコンピューティングを利用していると回答された方にお尋ねします。貴社でクラウドコンピューティングを導入するときに情報セキュリティ対策として確認ないし重視しているポイントをすべて選択してください。（○はいくつでも）

1 日本国内にサーバを設置している事業者を選択する　　2 データを定期的に自組織内にバックアップする
3 経済産業省や IPA のガイドラインに準拠した事業者を選択する　　4 「クラウドサービス安全・信頼性に係る情報開示認定制度」の認定事業者を選択する
5 事業者に対して情報セキュリティ監査を実施する　　6 情報セキュリティ対策として確認・重視すべきことはない
7 多重系、冗長系などのオプションサービスを契約する　　8 その他（　　）

Ⅱ．貴社における情報セキュリティ対策に関してお伺いします。

問 15 貴社では、「情報セキュリティ対策に取り組む基本的な方針」を公開していますか。（○は 1 つ）

※組織を対象とするセキュリティポリシーに相当します。個人情報の取扱いに関する方針の公開は含みません。

1 公開している　　2 公開していない

問 16 貴社には、CISO（Chief Information Security Officer：最高情報セキュリティ責任者）がいますか。（○は 1 つ）

1 専任者がいる　　2 兼任者がいる　　3 CISO はいない

問 17 貴社では、情報セキュリティ対策をどのような体制で行っていますか。（○は 1 つ）

1 専門部署（担当者）がある　　2 兼務だが担当責任者が任命されている

3 外部委託している　　4 組織的には行っていない（各自の対応）

5 わからない

→ 問 17-1 問 17 で組織的に情報セキュリティ対策を行っていると回答された方（1 または 2 と回答された方）にお尋ねします（以下、問 17-3 まで同じ）。セキュリティ対策部門の人数を専任・兼任別にお答えください。

a. 専任者 _____人　　b. 兼任者 _____人

→ 問 17-2 情報セキュリティ業務の担当者の量的な充足度について、もっともあてはまるものをお答えください。（○は1つ）また可能であれば、あと何人担当者[*3]がいればよいかについて、おおよその目安を記入してください。

1 十分である　　2 やや不足している　（およそ_____人程度の不足）

3 大幅に不足している（およそ_____人程度の不足）　　4 わからない

（*3） この場合の担当者とは、アップデート未実施機器の調査やユーザサポートのような通常時の対策業務を行うことができる担当者を指します。ウェブ改ざん等の原因究明に求められるような高度なスキルを有する必要はありません。

→ 問 17-3 情報セキュリティ業務の担当者のスキル面での充足度について、もっともあてはまるものをお答えください。（○は1つ）

1 十分である　　2 やや不足している

3 大幅に不足している　　4 わからない

問 18 貴社では、役職員等に対し、情報セキュリティ対策に関する教育をどのようにされていますか。役職・役割ごとに該当する教育手法の番号に○をご記入ください。（○は各行ともいくつでも）

	関連情報の周知	e ラーニング[*4]	外部講習会やセミナーの聴講	社内の自主的な勉強会	特に実施していない
a. 役員（経営トップを含む）	1	2	3	4	5
b. 情報セキュリティ管理業務の従事者	1	2	3	4	5
c. 正社員（a, b を除く）	1	2	3	4	5
d. 契約社員・アルバイト等	1	2	3	4	5

（*4） e ラーニングとは、パソコン、携帯端末等を使い、ネットワークや CD-ROM で教材を配信し、受講状況や成績の管理を伴う学習を想定しています。

問 19 情報セキュリティに関する事故や非常事態（大規模サイバー攻撃の発生等）への対応体制についてお尋ねします。貴社ではこうした状況が発生したときに、どのような体制で対応（外部組織との連絡等）していますか。（○は1つ）

1 コンピュータセキュリティインシデント（設問のような事故や非常事態）に対応する部門や人が定まっていない

2 特定の部門ではコンピュータセキュリティインシデントに対応する部門や人が定められている

3 上記の 2 に加え、コンピュータセキュリティインシデントに対して組織的に対策し、支援するチーム（CSIRT：コンピュータセキュリティインシデント即時対応チーム）を設置している

4 上記の 3 に加え、設置している CSIRT には DoS 攻撃[*5]等の外部要因のインシデント対応のために組織外部と調整する役割がある

5 わからない

（*5） DoS 攻撃とはサーバ等の情報システムを構成する機器に対して、故意に処理能力を大幅に超えるアクセスを行うこと等により、サービスの提供を阻害することを指します。非常に多数の拠点から同時集中的に攻撃を仕掛ける DDoS（分散型 DoS）などと呼ばれるものもあります。

問 20 貴社ではどのような情報セキュリティ関連製品やソリューションを導入していますか。

(1) 導入状況についてあてはまるものに○をご記入ください。(製品・ソリューション毎に○は1つ)。

(2) 2012 年度(2012 年 4 月～2013 年 3 月)新規導入の製品・ソリューションについて、2012 年度にセキュリティ上のトラブルを経験されなかった場合は 1、トラブルを経験された場合は、トラブル発生前に導入した場合は 2、発生後に導入した場合は 3 にそれぞれ○をご記入ください。ただし回答欄に数字のない項目については回答不要です。

	(1)導入状況			(2)トラブルの有無、導入の時期		
	2011 年度までに導入済	2012 年度新規導入	導入していない	2012 年度トラブルなし	2012 年度トラブルあり	
					トラブル発生前	トラブル発生後
a. セキュリティソフト(ネットワークサーバ向け)	1	2	3	1	2	3
b. セキュリティソフト(ローカルサーバ向け)	1	2	3	1	2	3
c. セキュリティソフト(クライアントパソコン向け)	1	2	3	1	2	3
d. プロバイダによるウイルスチェックサービス[*6]	1	2	3	1	2	3
e. ウェブ閲覧のフィルタリング	1	2	3	1	2	3
f. ネットワーク検疫システム[*7]	1	2	3	1	2	3
g. 下記 q、r 以外のアイデンティティ／ログオン管理製品(SSO[*8]等を含む)	1	2	3	1	2	3
h. 重要設備の多重化・冗長化	1	2	3	1	2	3
i. ポリシー/設定管理製品(情報漏えい対策製品、メール誤送信対策製品を含む)	1	2	3	1	2	3
j. ファイアウォール	1	2	3	(回答不要)		
k. Web アプリケーションファイアウォール(WAF)[*9]	1	2	3			
l. IDS[*10]/IPS による侵入検知	1	2	3			
m. データ(顧客情報等)の暗号化	1	2	3			
n. ISO/IEC15408[*11] 及び JCMVP/CMVP 認証取得製品やシステム	1	2	3			
o. VPN	1	2	3			
p. シンクライアント[*12]	1	2	3			
q. 生体認証(バイオメトリクス)	1	2	3			
r. IC カード・ワンタイムパスワード・PKI によるユーザ認証	1	2	3			
s. 資産管理ソフト(ライセンス管理ソフト)	1	2	3			
t. その他(　　)	1	2	3			

(*6) プロバイダによるウイルスチェックサービスには、アンチウイルスベンダーが提供するオンラインスキャンなども含めてください。

(*7) ネットワーク検疫システムとは、持ち込むパソコンを会社内 LAN に接続する際に、いったん別のネットワークに繋いでウイルスの検査等を行い、接続が許可されたパソコンであることを確認するシステムのことを指します。

(*8) SSO とは、シングルサインオンの略で、それぞれ独立した認証を要求する複数のコンピュータを、1回の認証手続きで利用できるようにするためのサービスのことです。

(*9) Web アプリケーションファイアウォール(WAF)とは、ウェブアプリケーションの脆弱性を悪用した攻撃などから ウェブアプリケーションを保護するソフトウエア、またはハードウエアです。WAF は脆弱性を修正するといった ウェブアプリケーションの実装面での根本的な対策ではなく、攻撃による影響を低減する対策です。

(*10) IDS とは、ネットワーク上などへの不正なアクセスの兆候を検知し、ネットワーク管理者に通報する機能のことです。 IPS とは、異常を通知するだけでなく、通信遮断などのネットワーク防御を自動で行う機能のことです。

(*11) ISO/IEC15408 とは、情報セキュリティの観点から IT 製品およびシステムの設計と実装に関して評価を行うための基準(国際標準)を指します。

(*12) シンクライアントとは、処理をサーバ側に集中させ、クライアントで必要最小限の処理のみを行うシステムを指します。ここではクライアントとしてパソコンなどを利用し、ファイルの保存をサーバのみで行う場合も含めてください。

問 21 情報セキュリティ関連被害を防止するために、どのような組織面・運用面の対策を実施していますか。

(1) 導入状況についてあてはまるものに○をご記入ください。(対策毎に○は1つ)。

(2) 2012 年度(2012 年 4 月～2013 年 3 月)新規導入の対策について、2012 年度にセキュリティ上のトラブルを経験されなかった場合は 1、トラブルを経験された場合は、トラブル発生前に導入した場合は 2、発生後に導入した場合は 3 にそれぞれ○をご記入ください。ただし回答欄に数字のない項目については回答不要です。

	(1)導入状況			(2)トラブルの有無、導入の時期		
	2011 年度までに導入済	2012 年度新規導入	導入していない	2012 年度トラブルなし	2012 年度トラブルあり	
					トラブル発生前	トラブル発生後
a. 機器や記録媒体の持込み・持出しの制限	1	2	3	1	2	3
b. 情報セキュリティ監査	1	2	3	1	2	3
c. セキュリティパッチの適用	1	2	3	1	2	3
d. 情報セキュリティ教育、研修	1	2	3	1	2	3
e. クラウドサービス利用における情報セキュリティに関わるルール・基準の策定・運用	1	2	3	1	2	3
f. パスワードの設定ルールの策定	1	2	3	1	2	3
g. IT インフラの構成や設定に関する文書化	1	2	3	1	2	3
h. ユーザの権限によるアクセス権限管理	1	2	3	(回答不要)		
i. フロアや施設への入退出管理	1	2	3			
j. 外部専門家によるセキュリティ監視サービスの導入	1	2	3			
k. ハードディスク等の廃棄時のデータ消去	1	2	3			
l. 事業継続計画(BCP)の策定	1	2	3			
m. 重要なシステム・データのバックアップ	1	2	3			
n. 情報セキュリティマネジメントシステム(ISMS)の認証取得	1	2	3			
o. プライバシーマーク(P マーク)の取得	1	2	3			
p. リスク分析に基づくリスク報告書の作成	1	2	3			
q. セキュリティポリシーの策定	1	2	3			
r. 情報の格付け(機密度レベルの設定)	1	2	3			
s. テレワーク・在宅勤務における情報セキュリティに関わるルール・基準の策定・運用	1	2	3			
t. 新たな製品やバージョンを導入する際の受入テストの実施	1	2	3			
u. その他(　　)	1	2	3			

問 22 問 20 に挙げたセキュリティ関連製品やソリューションの導入や問 21 で実施している対策について、2012 年度（2012 年 4 月～2013 年 3 月）にかけた費用[*13]を、それぞれ概算でわかる範囲でお答えください。（○は1つ）

1 1 百万円未満　2 1 百万円～5 百万円未満　3 5 百万円～1 千万円未満
4 1 千万円～2 千万円未満　5 2 千万円～5 千万円未満　6 5 千万円～1 億円未満
7 1 億円～4 億円未満　8 4 億円以上　9 わからない

（*13）セキュリティ対策用のソフトウエアのライセンス費用、ファイアウォール等のハードウエアの購入（レンタル・リース含む）費用、認証取得やアクセス管理といった運用面の対策費用を指します。導入や更新にかかる人件費は含めないでください。

問 22-1 問 22 で回答したもののうち、2012 年度のトラブル後に導入・実施したソリューションや対策がある場合は、その費用をわかる範囲でお答えください。（○は1つ）

1 1 百万円未満　2 1 百万円～5 百万円未満　3 5 百万円～1 千万円未満
4 1 千万円～2 千万円未満　5 2 千万円～5 千万円未満　6 5 千万円～1 億円未満
7 1 億円～4 億円未満　8 4 億円以上　9 わからない

問 22-2 2013 年度（2013 年 4 月～2014 年 3 月予定）に行うセキュリティ関連製品やソリューションの導入に要する費用は、問 22 で回答したものと比べてどのようになる見込みですか？（○は1つ）

1 増える　2 同程度　3 減る　4 未定

問 23 貴社では、Windows Update などの手段でサーバにセキュリティパッチ（脆弱性の修正）を適用していますか。最も近いものに○をご記入ください。（○は一列につき 1 つ）

	a. 外部に公開しているネットワークサーバ（メールサーバ、Web サーバなど）	b. 内部で利用しているローカルサーバ（ファイルサーバ、プリントサーバなど）
ほぼ全サーバに適用している	1	1
アプリケーションに影響がないことを確認できたもののみを適用している	2	2
情報セキュリティ対策上重要なもののみを適用している	3	3
ほとんど適用していない	4	4
外部事業者に運用を委託しているので、自ら適用する必要がない	5	5
該当するようなサーバを利用してない	6	6
わからない	7	7

問 23-1 問 23 の a. または b. で「ほとんど適用していない」を選んだ場合、セキュリティパッチを適用しない理由として、当てはまるものに○をご記入ください。（○はいくつでも）

1 パッチの適用が悪影響を及ぼすリスクを避けるため　2 パッチ適用以外の手段が有効であるため
3 パッチを適用しなくても問題ないと判断したため　4 パッチの評価や適用に多大なコストがかかるため
5 その他（　　）

問 24 貴社では、Windows Update などの手段でクライアント（パソコン）にセキュリティパッチ（脆弱性の修正）を適用していますか。最も近いものに○をご記入ください。（○は 1 つ）

1 常に適用し、適用状況も把握している　2 常に適用する方針・設定だが、実際の適用状況は不明
3 各ユーザに適用を任せている　4 ほとんど適用していない
5 わからない

問 25　貴社では、自社の資産や備品でない PC や外部記録媒体の社内ネットワークへの接続に関して、どのような方針のもとで運用していますか。最も近いものに○をご記入ください。（○は一列につき 1 つ）

		a. 自社資産以外の PC の接続（私物ノート PC 等）	b. 自社備品以外の外部記録媒体の接続（私物 USB メモリ等）
禁止している	セキュリティ担当者が状況を監視している	1	1
	セキュリティ担当者が状況を監視していない	2	2
届け出に応じた許可制としている		3	3
禁止していない		4	4
その他 （　　）		5	5

問 26 貴社では、セキュリティインシデントの原因となった従業員に対し、どのような措置を行っていますか。あてはまるものに○をご記入ください。（○はいくつでも）

1　罰則の適用（人事面での処遇見直し、減給等）
2　インシデントの経緯について公式な形で社内に連絡する（個人名を明示する）
3　インシデントの経緯について公式な形で社内に連絡する（個人名を明示しない）
4　本人に文書で注意する
5　本人の上司に文書で注意する
6　本人に口頭で注意する
7　本人の上司に口頭で注意する
8　その他（　　）
9　特に何もしない

問 27 情報セキュリティ対策の必要性を感じたきっかけは何ですか。該当するものを下記よりすべてお選びください。（○はいくつでも）

1　法令（個人情報保護法等）の制定
2　業界基準の制定
3　重要情報（個人情報、営業秘密、技術情報等）の保持
4　取引先からの要請
5　自社のセキュリティ事故
6　他社のセキュリティ事故
7　対外（取引先、ユーザ等）へのアピール
8　セキュリティベンダーからの勧奨
9　同業他社の対策状況をみたこと
10　その他（具体的に:　　）
11　対策の必要性を感じたことがない

以降の設問では、2012 年度（2012 年 4 月～2013 年 3 月）に貴社が直面した情報セキュリティ関連の脅威と被害について伺います。
脅威は「コンピュータウイルス」「ウイルス以外のサイバー攻撃等」の 2 種類です。

それぞれの脅威について、被害経験に関する設問（問 28、問 34、問 35）については全員がお答えください。
被害経験がある場合は、被害経験のある脅威について、被害の内容に関する設問にお答えください。
被害経験のない脅威については、被害の内容に関する設問に回答いただく必要はありません。

	被害経験（全員回答）	被害内容（被害経験がある場合のみ回答）
コンピュータウイルス	問 28	問 29～問 33（損失に関する設問　問 38～問 47）
ウイルス以外のサイバー攻撃等	問 34、問 35	問 36～問 38（損失に関する設問　問 38～問 47）

Ⅲ.「コンピュータウイルス」についてお伺いします。

問 28 貴社では、2012 年度 1 年間（2012 年 4 月～2013 年 3 月）に、コンピュータウイルス[*14] に感染したことがありましたか。一度でもあればお答えください。（○は 1 つ）

＊ 傘下事業所（支社・支店・出張所等）も含めてご回答ください。

1　ウイルスに感染した	2　ウイルスを発見したが、感染には至らなかった
3　ウイルスをまったく発見しなかった	4　わからない

（*14）コンピュータウイルスとは、第三者のプログラムやデータベースに対して意図的に何らかの被害を及ぼすように作られたプログラムであり、自己伝染機能、潜伏機能、発病機能の 3 つの機能のうち、ひとつ以上を有するものです。

【問28で「1 ウイルスに感染した」あるいは「2 ウイルスを発見したが、感染には至らなかった」と答えた方は、引き続き問29へお進みください。「3 ウイルスをまったく発見しなかった」あるいは「4 わからない」と答えた方は、問34へお進みください。】

問29 コンピュータウイルスを発見した方法について、該当するものをすべてお選びください。(○はいくつでも)

1 ウイルス対策ソフト(クライアント型)　2 ウイルス対策ソフト(ゲートウェイ型)
3 プロバイダのチェックサービス　4 ファイアウォール
5 IDS、IPSによる侵入検知　6 挙動の異常等から
7 外部からの連絡　8 その他 (　　)

問30 感染あるいは発見したコンピュータウイルスの侵入経路はどのように想定されますか。(○はいくつでも)

1 電子メール　2 インターネット接続 (ホームページ閲覧など)
3 自らダウンロードしたファイル　4 P2P(Peer to Peer)などのファイル共有ソフト
5 USBメモリ等の外部記憶媒体　6 持ち込みクライアント(パソコン)
7 その他 (　　)　8 わからない

【問 28 で「1 ウイルスに感染した」と答えた方は、引き続き問 31 へお進みください。「2 ウイルスを発見したが、感染には至らなかった」と答えた方は、問34へお進みください。】

問31 2012年度1年間(2012年4月～2013年3月)にコンピュータウイルス感染が発生した回数をお答えください。
複数の感染がほぼ同時期に発生した場合、ウイルスの種類・感染源が同じと想定される場合はまとめて1回と数えます。(感染したクライアント、サーバの台数は次の問32でお答えください)。

＿＿＿＿＿＿＿＿回 / 年

問32 ウイルスに感染したクライアント(パソコン)、サーバ、スマートフォン・タブレット端末の台数は年間延べ何台ですか。それぞれについて台数を概算でご記入ください。

a. クライアント(パソコン) ＿＿＿＿＿＿台 / 年　b. サーバ ＿＿＿＿＿＿台 / 年
c. スマートフォン・タブレット端末 ＿＿＿＿＿＿台 / 年

問33 ウイルスに感染した影響で生じた直接的な被害に、あてはまるものをお答えください。(○はいくつでも)

1 情報破壊　2 情報漏洩　3 ウイルスメール等の発信
4 ネットワークの遅延　5 システム停止・性能低下　6 パソコン単体の停止
7 関連部門の業務停滞　8 個人の業務停滞　9 取引先への感染拡大
10 その他(　　)　11 特になし

Ⅳ.「ウイルス以外のサイバー攻撃等」についてお伺いします。

問34 貴社では、2012年度1年間(2012年4月～2013年3月)に、自社のサーバやクライアント(パソコン)についてサイバー攻撃(不正アクセス[*15]、DoS攻撃、標的型攻撃[*16]など)にあったことがありましたか。一度でもあればお答えください。(○は1つ)

＊ 傘下事業所(支社・支店・出張所等)も含めてご回答ください。

1 サイバー攻撃で被害にあった	2 サイバー攻撃を受けたが、被害には至らなかった
3 サイバー攻撃をまったく受けなかった	4 わからない

(*15) ここでは不正アクセスとは、インターネットを介して外部から、サーバやクライアント(パソコン)を許可なく操作し、不正に情報を読み取る、情報を書き換える、削除するなどの行為すべてを含むものとします。最近の事例としては、Webサイトの改ざん、機密情報の漏洩などが報告されています。

(*16) 標的型攻撃とは、主に電子メールを用いて特定の組織や個人を狙う手法です。典型的な例として、メール受信者の仕事に関係しそうな偽の話題等を含む本文や件名で騙し、添付ファイル(ウイルス等)のクリックを促す手口が知られています。広告やフィッシング詐欺などを狙い、受信者の意図に反して無差別かつ大量に送信される「スパムメール」とは区別します。

問 35 貴社では、2012 年度 1 年間(2012 年 4 月～2013 年 3 月)に、内部者(委託者を含む)の不正に起因する情報漏洩やシステムの悪用等の情報セキュリティ上のトラブルがありましたか。一度でもあればお答えください。(○は 1 つ)

＊ 傘下事業所(支社・支店・出張所等)も含めてご回答ください。

1 内部者(委託先を含む)の不正による被害があった
2 内部者(委託先を含む)の不正による被害はなかった
3 わからない

【問 34 で「1 ウイルス以外のサイバー攻撃で被害にあった」あるいは「2 ウイルス以外のサイバー攻撃を受けたが、被害には至らなかった」と答えた方は、問 36 へお進みください。「3 ウイルス以外のサイバー攻撃をまったく受けなかった」あるいは「4. わからない」と答えた場合、問28で「1 ウイルスに感染した」と答えた方は12ページ問38へ、それ以外の回答の方は15ページ問48へお進み下さい。】

問 36 貴社が受けたサイバー攻撃の手口にあてはまるものをお答えください(○はいくつでも)

1 ID・パスワードを騙し取られてユーザになりすまされたことによる不正アクセス
2 脆弱性(セキュリティパッチの未適用)を突かれたことによる不正アクセス
3 SQL インジェクション*17
4 DoS 攻撃
5 標的型攻撃
6 その他(　　)
7 手口はわからない

(*17) SQL インジェクションとは、細工された SQL 文を Web サイトの入力欄に埋め込み、データベースを不正に操作する手法です。

問 36-1 問 36 で「5 標的型攻撃」を受けたとお答えの方にお伺いします。(以下、問 36-2 も同じ)。標的型攻撃による被害の状況をお答えください。(○は 1 つ)

1 標的型攻撃を発見した(のみ)
2 標的型攻撃が原因と考えられるウイルス感染、不正アクセス、情報漏洩等が確認された

問 36-2 攻撃の具体的な手段についてご記入ください。(○はいくつでも)

1 同僚や取引先、サービス事業者からのメールを装い、添付したウイルスファイルを開かせる
2 公的機関からのメールを装い、添付したウイルスファイルを開かせる
3 製品やサービスの顧客を装い、ウイルスファイル付きの相談メールを相談窓口等に送りつける
4 電子メールに表示された URL 経由で攻撃用のウェブサイトに誘導される
5 その他(　　)

問 36-3 貴社が 2012 年度 1 年間(2012 年 4 月～2013 年 3 月)に受信した標的型攻撃と思われる電子メールの数をご記入ください。(スパムメールは含めないでください)

合計:(　　)通／年 程度

【問 34 で「1 ウイルス以外のサイバー攻撃で被害にあった」と答えた方は、引き続き問 37 へお進みください。問 34 で「2 ウイルス以外のサイバー攻撃を受けたが、被害には至らなかった」と答えた方のうち、問 28 で「1 ウイルスに感染した」と答えた方は 12 ページ問 38 へ、それ以外の回答の方は 15 ページ問 48 へお進みください。】

問 37 貴社が受けたサイバー攻撃の被害に、あてはまるものをお答えください。(○はいくつでも)

1 Web サイトが改ざんされた
2 Web サイトから情報(顧客情報、業務情報等)が盗まれた(流出した)
3 Web サイトのサービスが停止させられた
4 Web サイトのサービスの機能が低下させられた
5 業務サーバの内容が改ざんされた
6 業務サーバから情報(顧客情報、業務情報等)が盗まれた(流出した)
7 業務サーバのサービスが停止させられた
8 業務サーバのサービスの機能が低下させられた
9 貴社が提供するネットサービスにおいて、第三者のなりすましによる不正使用があった
10 取引先の企業や個人に被害が拡大した
11 その他(　　)

Ⅴ.「被害により生じた直接的損失」についてお伺いします。

【問 38～問 47 は、問 28 で「1 ウイルスに感染した」と答えた方、または、問 34 で「1 ウイルス以外のサイバー攻撃で被害にあった」と答えた方のみお答えください。それ以外の方は、15 ページ問 48 へお進みください。】

問 38 電子商取引(EC)業務を行っている方(問 9 で 0%以外を選択された方)にお聞きします。ウイルス感染やサイバー攻撃(ウイルス以外)を受けた影響によって、電子商取引(EC)が停止した期間は年間延べ何日ですか。(○は 1 つ)

1 停止していない　2 4 時間未満　3 4～8 時間未満　4 8～12 時間未満
5 12～24 時間未満　6 24 時間～3 日未満　7 3～6 日未満　8 6 日以上(具体的に　日)

問 39 ウイルス感染やサイバー攻撃(ウイルス以外)を受けた影響によって、EC 関連以外の業務遂行上重要なサーバが停止した期間は年間延べ何日ですか。(○は 1 つ)
＊ 傘下事業所(支社・支店・出張所等)も含めてお答えください。

1 停止していない	2 4 時間未満	3 4～8 時間未満	4 8～12 時間未満
5 12～24 時間未満	6 24 時間～3 日未満	7 3～6 日未満	8 6 日以上(具体的に　日)

→ 問 39-1 問 39 で「停止した」と回答された方にお尋ねします。EC 関連以外の業務遂行上重要なサーバが停止したことで、貴社の商取引が中断[*18]しましたか。(EC 業務における商取引の中断は除きます)(○は 1 つ)

1 中断した　2 中断しなかった　3 わからない

(*18) ここで「商取引の中断」とは、サーバの停止の結果、受発注、決済などの業務が停止してしまうことを指します。

→ 問 39-2 問 39-1 で「中断した」と回答された方にお尋ねします(以下、問 39-4 まで同じ)。商取引が中断したのは、サーバ停止からどの程度時間が経過した頃でしたか。(○は 1 つ)

1 サーバ停止直後　2 4 時間未満　3 4～8 時間未満　4 8～12 時間未満
5 12～24 時間未満　6 24 時間～3 日未満　7 3～6 日未満　7 6 日以上 (　日)

→ 問 39-3 貴社の、EC 関連以外の業務遂行上重要なサーバについて、売上高に影響を及ぼさないで済む最長の停止時間(許容停止時間)はどれくらいでしょうか。最も近いものに○をご記入ください。(○は 1 つ)

1 ごくわずかな停止も影響を及ぼす　2 4 時間未満　3 4～8 時間未満
4 8～12 時間未満　5 12～24 時間未満　6 24 時間～3 日未満
7 3～6 日未満　8 6 日以上(具体的に　日)　9 わからない

→ 問 39-4 貴社の、EC 関連以外の業務遂行上重要なサーバが営業日に「24 時間」停止した場合、貴社のその日の売上高にどの程度の影響を及ぼしますか。最も近いものに○をご記入ください。(○は 1 つ)

1 ほとんど影響を受けない(25%減未満)　2 影響はあるが部分的にとどまる(25%減以上～50%減未満)
3 大きな影響を受ける(50%減以上～75%減未満)　4 深刻な影響を受ける(75%減以上)
5 わからない

問 40 情報管理部門が行ったウイルス感染やサイバー攻撃（ウイルス以外）の被害からの復旧作業[*19] にはどの程度の人員と時間を要しましたか。（○はそれぞれ 1 つ）

投入した要員数	1 作業せず	2 1 人	3 2～3 人	4 4～5 人
	5 6～10 人	6 11～15 人	7 16～20 人	8 21 人以上（　　人）
要した時間	1 作業せず	2 4 時間未満	3 4～8 時間未満	4 8～12 時間未満
	5 12～24 時間未満	6 24 時間～3 日未満	7 3～6 日未満	8 6 日以上（　　日）

（*19） ここでは、ウイルス感染やサイバー攻撃の事実を確認した後の作業のことをいい、具体的には、被害原因を特定し、システムに必要な修正等を行い、ウイルス感染やサイバー攻撃の原因を取り除くといった作業を指します。

問 41 ウイルス感染やサイバー攻撃（ウイルス以外）の被害からのシステム復旧に関して新たに購入（レンタル・リース含む）した代替機器の費用[*20]をお答えください。（○は 1 つ）

1 0 円　　2 10 万円未満　　3 10～30 万円未満
4 30～50 万円未満　　5 50～70 万円未満　　6 70～100 万円未満
7 100～200 万円未満　　8 200～300 万円未満　　9 300 万円以上（　　万円 / 年）

（*20） 一時的に利用するために事後に購入したハードウエアやソフトウエアの費用のみを指します。 恒久的な対策強化を目的に購入した機器の費用は含めないでください。

問 42 ウイルス感染やサイバー攻撃（ウイルス以外）の被害からのシステム復旧に関し、システム構築等で外部に発注した業務の費用をお答えください。（○は 1 つ）

1 0 円　　2 10 万円未満　　3 10～30 万円未満
4 30～50 万円未満　　5 50～70 万円未満　　6 70～100 万円未満
7 100～200 万円未満　　8 200～300 万円未満　　9 300 万円以上（　　万円 / 年）

問 43 ウイルス感染やサイバー攻撃（ウイルス以外）の被害により、業務部門が行った追加のデータ処理作業[*21] にはどのくらいの人員と時間を要しましたか。（○はそれぞれ 1 つ）

投入した要員数	1 作業せず	2 1 人	3 2～3 人	4 4～5 人
	5 6～10 人	6 11～15 人	7 16～20 人	8 21 人以上（　　人）
要した時間	1 作業せず	2 4 時間未満	3 4～8 時間未満	4 8～12 時間未満
	5 12～24 時間未満	6 24 時間～3 日未満	7 3～6 日未満	8 6 日以上（　　日）

（*21） ここでは、ウイルス感染やサイバー攻撃が原因で消失したデータの再登録や、一時的に手作業等で作成したデータのシステムへの登録などの作業を指します。

問 44 ウイルス感染やサイバー攻撃（ウイルス以外）時の対応として実施した内容について該当する番号に○をご記入ください。また、貴社内で発生したおおよその作業規模をお答えください。（○はいくつでも）「5 その他」の場合は、できるだけその内容をご記入ください。

		社内で発生した作業の規模 投入要員数	社内で発生した作業の規模 一人あたり平均所要時間
1 原因追求・影響範囲特定のための調査	⇒	約＿＿＿人	約＿＿＿時間
2 問合せ窓口（コールセンター）の設置	⇒	約＿＿＿人	約＿＿＿時間
3 取引先・顧客等への謝罪（金券等を含む）	⇒	約＿＿＿人	約＿＿＿時間
4 謝罪広告の出稿	⇒	約＿＿＿人	約＿＿＿時間
5 代替設備・サービス等の手配	⇒	約＿＿＿人	約＿＿＿時間
6 サーバや PC の再インストール・設定等	⇒	約＿＿＿人	約＿＿＿時間
7 その他（　　）	⇒	約＿＿＿人	約＿＿＿時間
8 特に実施していない	⇒	約＿＿＿人	約＿＿＿時間

問 45 ウイルス感染やサイバー攻撃（ウイルス以外）を受けたことによって生じた間接的な被害にあてはまるものに、○をご記入ください。（○はいくつでも）

1 顧客が減少した、顧客から指名停止を受けた
2 取引先から補償・補填を求められた
3 関係者から訴訟を起こされた
4 インターネット上で中傷されたり、流言を流された
5 その他（ ）
6 特に間接的な被害は受けなかった

問 46 2012 年度 1 年間（2012 年 4 月～2013 年 3 月）に、ウイルス感染やサイバー攻撃（ウイルス以外）を受けたことに対する対応として実施した内容のうち、原因・被害範囲の調査、対策の見直し作業等の目的で外部（セキュリティサービスベンダ、コンサルタント等）に発注した業務の費用をお答えください。（実施していない場合は「0 円」を選択してください。○は 1 つ）

1 0 円
2 10 万円未満
3 10～100 万円未満
4 100～300 万円未満
5 300～500 万円未満
6 500～1,000 万円未満
7 1,000 万円以上（ 万円 / 年）

問 47 貴社では、自社で経験したウイルスやサイバー攻撃の被害について、被害内容や対応状況に関する情報を外部に公開しましたか。（○は 1 つ）

1 公開した
2 公開しなかった

問 47-1 「1. 公開した」を選択された方にお聞きします。公開した情報は、どのような媒体に掲載されましたか。（○はいくつでも）

1 自社のホームページに掲載した
2 新聞や雑誌に掲載された
3 ウェブニュースに掲載された
4 ネットの掲示板に書き込まれた
5 その他（ ）

Ⅵ. ヒアリングへのご協力について

問 48 （全員にお伺いします）貴社のセキュリティ対策や情報セキュリティ関連事象について、本アンケートとは別に、IPA からヒアリングをお願いした場合、ご協力いただくことは可能ですか。（○は1つ）

1　協力してもかまわない　　2　協力はできない

16 ページの「個人情報のお取り扱いについて」にご同意の上、差し支えない範囲でご記入をお願いいたします。

貴社・貴事業所名	
所属部署・役職	
お名前	
ご住所	
E-mail アドレス	
詳細結果希望	1 希望する　　2 希望しない

※ご回答くださった方には、独立行政法人情報処理推進機構（IPA）サイトにおける調査結果の公表を電子メールにてご案内させていただきます。また、上記「詳細結果希望」に「1　希望する」に○をつけた方には、今回のアンケート調査における企業の回答傾向の中で、貴社の状態がわかる詳細資料を電子メールにてお送りいたします。

【モニタ登録のお願い】

- 独立行政法人 情報処理推進機構（IPA）では、今後も本調査を継続的かつ安定的に実施するために、本調査にご回答くださった方の中から、次年度の調査にご協力いただけるモニタとしてご登録いただける方を募集しています。
- 具体的には、以下の方法によりモニタ登録してくださった方のご連絡先情報を IPA 内で適切に管理し、次年度の調査時に本調査票を直接送付させていただきます。つきましては、可能な範囲で本年同様に調査にご協力いただければ幸いです。
- モニタ登録してくださった方には、御礼として「情報セキュリティ白書 2013」（2013 年 9 月発行予定）を差し上げます。

（参考）
プライバシーポリシー（独立行政法人 情報処理推進機構）
http://www.ipa.go.jp/about/privacypolicy/

● モニタ登録の方法

IPA の次のメールアドレスに、下記の情報を記載した電子メールをお送りください。その電子メールが、モニタ登録の申込になります。

（宛　先）　isec-survey@ipa.go.jp
（件　名）　モニタ登録について
（必要事項）　・貴社・貴事業所名
・御所属部署・御役職
・御住所
・御担当者御氏名
・E-mail アドレス
・貴社従業員数（単体）

ご協力ありがとうございました

個人情報のお取り扱いについて

みずほ情報総研株式会社

本アンケートは、独立行政法人情報処理推進機構より委託を受けてみずほ情報総研株式会社が実施するもので、経済産業省「情報処理実態調査」対象企業、帝国データバンク登録企業から無作為に抽出した企業、及び独立行政法人情報処理推進機構が過去に実施した「情報セキュリティ事象被害状況調査」のモニタの方にお送りしています。

ご回答者の個人情報のお取り扱いについては、下記の通り適切に管理いたしますので、ご同意の上、アンケートにご回答くださいますようお願い申し上げます。

１．個人情報の取扱いに関する弊社の基本姿勢

みずほ情報総研株式会社は、プライバシーマークの付与･認定を受けております。ご回答者の個人情報は、弊社が定める「個人情報保護方針」に則り、適切な保護措置を講じ、厳重に管理いたします

２.ご回答者の個人情報の利用目的

ご回答者の個人情報は、企業における情報セキュリティ関連被害等の状況調査に関して、(1) IPA サイトにおける調査結果公表についてのご案内、(2)調査票ご提出後の回答内容の確認・再調査のご依頼、を行うために利用させていただきます。本目的以外の目的で個人情報を利用する場合は、改めて目的をお知らせし、同意を得るものといたします。

３．ご回答者の個人情報の委託・提供

ご回答者の個人情報につきまして、外部委託事業者に個人情報を取扱う業務（調査票の発送、調査票の回収・集計・調査票の督促業務・回答内容の確認）を委託致します。その際、必要な契約を締結し、弊社の従業員に対するのと同等の管理を行います。また、ご回答者の個人情報は、調査票回答内容の確認、再調査のために、委託元である独立行政法人情報処理推進機構へ提供いたします。
独立行政法人情報処理推進機構のプライバシーポリシーは以下をご覧ください。
http://www.ipa.go.jp/about/privacypolicy/index.html

４．ご回答者の個人情報の利用目的終了後の措置

ご回答者の個人情報は、当該利用目的終了後、当社管理分については、責任を持って適切に廃棄いたします。

５．個人情報に関するご連絡先

① 個人情報保護管理者：みずほ情報総研株式会社 経営・IT コンサルティング部　部長 川添祥宏
② 個人情報の取扱いに関するご連絡先、苦情・相談窓口
※開示、訂正、利用停止等のお申し出は、下記窓口までご連絡ください。

みずほ情報総研株式会社　経営・IT コンサルティング部　冨田・能瀬・小川・築島
電話：03-5281-5492　FAX：03-5281-5429
E-mail：sec-enq@mizuho-ir.co.jp
URL：http://www.mizuho-ir.co.jp/privacy/policy.html