（３） キーリカバリー機能の必要性

・キーリカバリー機能の必要性については、３６３社中、必要とする企業が１６４社（４５．２％）、必要としない企業が４３社（１１．８％）となっているが、「わからない」とする企業も１５１社（４１．６％）ある。

・キーリカバリーが必要となる場合については、１６４社中、「社員が急に退職・死亡したとき」とする企業が１０５社（６４．０％）、「鍵を消失してしまったとき」とする企業が１０４社（６３．４％）、「不正利用等が行われた時にチェックするため」とする企業が８９社（５４．３％）、「情報の内容に問題がないかどうかを常にチェックするため」とする企業が４８社（２９．３％）等となっている。

問. キーリカバリー機能（利用者から暗号鍵の保管・管理を委託され、利用者の求めに応じて鍵の回復を行う機能）は必要だと思われますか？ 下記のうち該当するもののいずれか1つに○をお付け下さい。

（　　）①思わない
（　　）②わからない
（　　）③思う

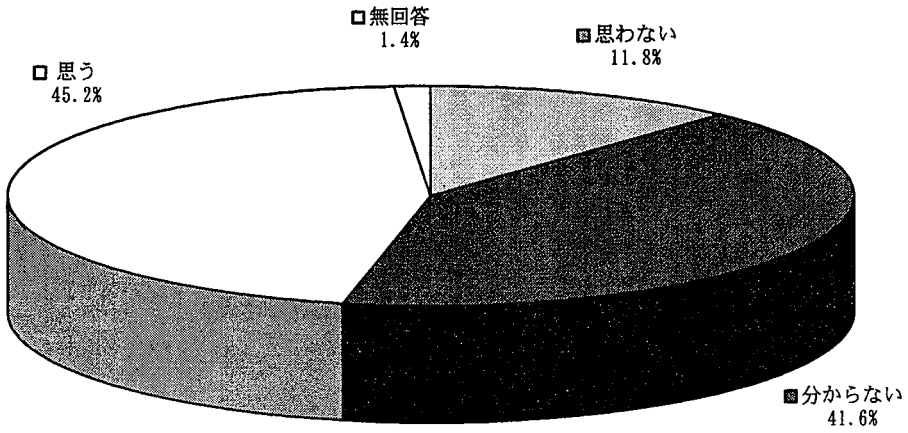
---

(1)集計結果

Q16 キーリカバリー機能の必要性	回答数	構成比1	構成比2
思わない	43	11.8%	11.8%
分からない	151	41.6%	41.6%
思う	164	45.2%	45.2%
無回答	5	1.4%	1.4%
回答数	363		
回答対象社数	363		

構成比１…その選択肢を選んだ社数／総回答数（得票総数に対するその選択肢のシェアを示す。）
構成比２…その選択肢を選んだ社数／回答すべき対象社数（その選択肢の支持率を示す。）

(2)構成比１グラフ



問．どのような場合に必要になるとお考えですか？下記のうち該当するものにいくつでも○をお付け下さい。

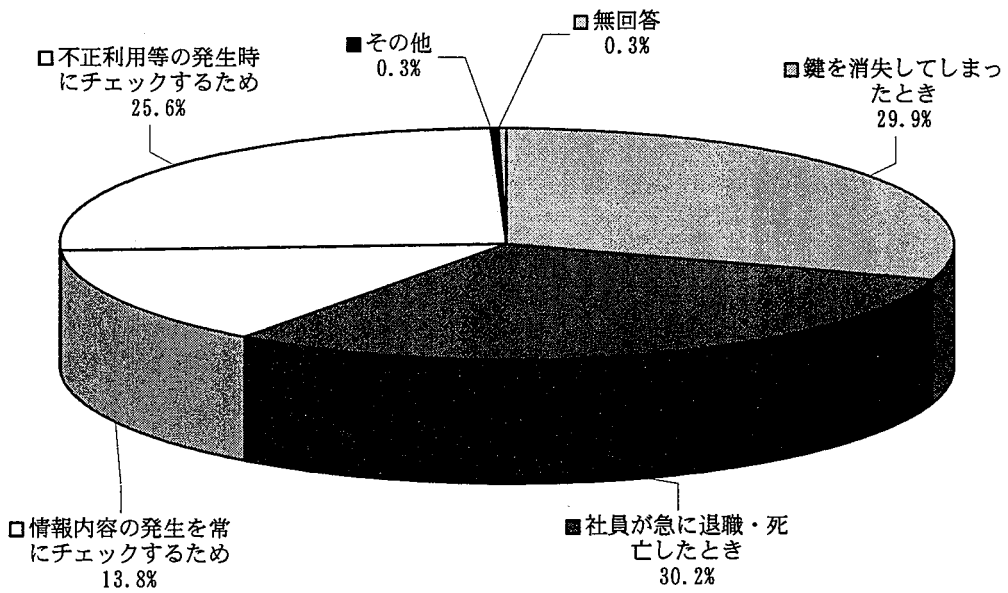
(　　)①鍵を消失してしまったとき
(　　)②社員が急に退職・死亡したとき
(　　)③情報の内容に問題がないかどうかを常にチェックするため
(　　)④不正利用等が行われた時にチェックするため
(　　)⑤その他（　　）

(1)集計結果

Q16-1 ｷｰﾘｶﾊﾞﾘｰが必要になる場合	回答数	構成比1	構成比2
鍵を消失してしまったとき	104	29.9%	63.4%
社員が急に退職・死亡したとき	105	30.2%	64.0%
情報内容の問題点を常にチェックするため	48	13.8%	29.3%
不正利用等の発生時にチェックするため	89	25.6%	54.3%
その他	1	0.3%	0.6%
無回答	1	0.3%	0.6%
回答数	348		
回答対象社数	164		

構成比1…その選択肢を選んだ社数／総回答数（得票総数に対するその選択肢のシェアを示す。）
構成比2…その選択肢を選んだ社数／回答すべき対象社数（その選択肢の支持率を示す。）

(2)構成比1グラフ



5　政府等に対する情報セキュリティに関する要望事項

・政府、メーカー、ネットワーク関連企業等に対する要望等について、フリーアンサー形式での回答を求めたところ、その回答は、おおむね次の４項目にまとめることができる。

（１）暗号技術に関するもの

「長期間使える１つの方式に統一する。」

「認証機関不要の暗号化技術の開発・ファイアウォール間の暗号化技術の標準化（ハード、ソフトに左右されないもの）」

「標準化と仕様統一を行い、それでもセキュリティを保てる技術の確立」

等８件

互換性の確保や利便性の観点から、規格や仕様の統一、標準化を求める要望が多かった。

（２）情報公開及び啓蒙に関するもの

「インターナショナルにポリシーを示し、運営する機関を設立し、情報公開に努め安心して利用できるようにして欲しい。」

「各種情報の開示・被害事例の紹介、啓蒙」

「ユーザー側に有益な情報を平易に流してほしい。」

「不正が行われた場合の速やかな開示」　等５件

犯罪等による被害の事例、ネットワーク関連企業等のセキュリティ対策等各種情報を開示することによって、ユーザーが利用しているネットワークの安全性を十分認識した上で、安心して利用することができるように情報公開や啓蒙活動の活発化を求める意見が多かった。

（３）規制や法整備に関するもの

「インターネット利用によるデータの信頼性を確保するため行政等からの規制を至急実施する必要がある。」

「ネットワーク上にあろうとなかろうと犯罪抑止のための法整備は必要である。併せて最新技術のサポートも必要であり、政府・メーカーの相互協力体制を望む。」　等６件

情報セキュリティを確保するためのルール作りを求めるとともに、ネットワーク上の不正行為の処罰を求める要望が多かった。

（４） 認証機関の位置付けに関するもの

「現在は各認証機関がばらばらに認証を行っているので、個々の認証機関毎に証明をとる必要がある。公的な認証として管理すべきと考える。」

「公正な立場で使用者が安心して使用できる標準を打ち出してほしい。」

「認証機関に許認可を与え、指導監督する行政機関の早期明確化。セキュリティ保護のための法整備（刑事罰の規定も含む）」

「認証機関はいわゆる公証人であるので、許認可までは不要だが、業として行う限り不正等に対して刑事罰が設けられるような立法が必要と思う。」　等９件

認証機関を許可制にすることに関しては賛否両論あるが、信頼性の確保及び標準化に向けての何らかの施策を求めている意見が多かった。

第３章　情報セキュリティ対策の課題と暗号技術の普及を図る施策の在り方

１　企業等の情報セキュリティ対策の現状と課題

（１）企業等の情報セキュリティ対策の現状と問題点

第２章２（２）イ及び第２章３（２）イの調査結果から、企業内や企業間でのデータのやり取り及びネットワークを使った一般消費者との情報のやり取りに関するセキュリティ対策の現状について、多くの企業が不安を感じている状況がうかがえる。また、第２章（２）アにおける企業等の情報セキュリティ対策についての関心の状況にかんがみると、不安を感じていない企業についても、情報セキュリティに関する意識が低いために、不安を感じていないものと考えられる。

さらに多くの企業が感じている不安の内容としては、企業内や企業間でのデータのやり取りについては、「社員が不正にデータを持ち出すかもしれない。」といった内部不正、「社員になりすましてデータを盗用されるかもしれない。」といった「なりすまし」及び「やりとりするデータを盗聴されるかもしれない。」といった盗聴が、また、一般消費者との情報のやりとりについては、「他人になりすまして不正な注文が発生する」といった「なりすまし」や、「顧客のクレジットカード番号が盗用される」、「顧客情報（クレジットカード番号以外）が盗聴される」といった盗聴が挙げられており、ネットワーク社会における「本人確認」及び「情報の保護」の重要性を裏付ける結果となっている。

しかしながら、企業等の情報セキュリティ対策の実施状況について見ると、第２章２（１）イ、３（２）ア、４（１）及び（２）の調査結果から、売上情報、商品・価格情報、顧客情報、企画書・提案書、人事情報、顧客等の重要データや、クレジットカード番号、銀行口座、年収等の顧客に関する情報のやりとりについては、インターネットを利用しない、あるいは、データ交換そのものを差し控えるといった対応をする傾向がみられ、認証（「本人確認」）機能及び秘匿（「情報の保護」）機能を有し、「なりすまし」や盗聴等のネットワークに係る不正行為に対して有効とされている暗号技術、認証機関を利用している企業等の割合は、それぞれ、約１０％（３６３社中３７社）、約５％（３６３社中１９社）と、その利用状況は

極めて低調であり、情報セキュリティに対する不安がセキュリティ対策の実施状況に結び付いておらず、セキュリティ対策が低調である状況が明らかとなっている。

そして、暗号技術又は認証機関を利用しない理由としては、「必要性を感じない」とする企業が暗号技術について、約２８％（３０６社中８４社）、認証機関についても、約２８％（１８８社中５２社）という結果となっており、情報セキュリティ対策の必要性及び情報セキュリティ対策における暗号技術利用の有用性についての理解が十分でない状況が認められる。その他の理由としては、暗号技術について、「利用方法が分からない」とする企業が約２１％（３０６社中６５社）、「多種多様な方法があるなど、利用が面倒である」とする企業が約２０％（３０６社中６２社）、認証機関について、「利用方法が分からない」とする企業が約２２％（１８８社中４１社）、「複数の機関があるなど、利用が面倒である」とする企業が約１５％（１８８社中２８社）という結果となっており、現在利用されている暗号技術及び認証機関の利用しにくさが暗号技術及び認証機関の利用の普及の妨げとなっている状況がうかがえる。

以上のことから、企業等における現状の情報セキュリティ対策が低調である原因としては、次の２つが挙げられ、今後、企業等における情報セキュリティ対策を促進するためには、この２つの問題点を早急に解決していく必要がある。

①企業等の情報セキュリティ意識の低さ（情報セキュリティに関する意識及び危機感の欠如）

②暗号技術及び認証機関の利用のしにくさ

（２） 企業等の情報セキュリティ対策の課題

我が国社会の急速なネットワーク社会化に伴い、電子商取引（ネットワーク上で買物などのサービスの利用や支払いをすること。ＥＣ（Electronic Commerce）ともいう。）や電子マネーの実証実験が盛んに進められており、その本格的な実用化も間近なものと期待されている状況にあり、今後、企業等がその事業活動においてインターネット等のオープンネットワークを利用する機会がますます増大することが予想される。したがって、多く

の企業等が行っている重要なデータ交換について、ネットワークの利用をしないという消極的な対応を今後とも続けることは困難と考えられ、本格的な情報セキュリティ対策を講ずる必要があると考えられる。仮に、現状のようなセキュリティ対策のままで、企業等がその事業活動に本格的にオープンネットワークを利用し始めた場合には、盗聴、「なりすまし」等のネットワークに係る不正行為に十分対応できず、犯罪等が多発し、ネットワーク社会化の進展自体を阻害する結果にもなりかねず、ひいては日本経済の発展を阻害するおそれもある。

そして、これら「なりすまし」や盗聴等のネットワークに係る不正行為に十分対応でき、安心して十分にネットワークを利用するためには暗号技術の利用が有効であり、暗号技術の利用が今後ますます必要かつ重要となる。

以上のようなことから、企業等における情報セキュリティ対策の問題点を解決し、これを促進するためには、次の２つの課題の解決を図ることにより、暗号技術の普及を図っていく必要がある。

①企業等の情報セキュリティ意識（情報セキュリティ対策の必要性及び情報セキュリティ対策における暗号技術利用の必要性・重要性等に対する意識）を高めること。

②利用しやすい暗号製品等の開発・普及及び利用しやすい認証機関の整備を推進すること。

2　暗号技術の普及を図る施策の在り方

（１）企業等の情報セキュリティ意識の高揚方策

ア　広報啓発活動の強化

（ア）　広報啓発活動の必要性

盗聴、「なりすまし」等のネットワークに係る不正行為を防止するため、良質な暗号技術の普及を図る必要があるが、そのためには、ネットワークを利用するすべての者が情報の漏洩、盗聴、改ざんやなりすましによる犯罪等ネットワークの利用に係るリスクを自らにかかわる問題として認識するとともに、これらのリスクを回避するために

は、暗号技術を利用することが必要であることを認識することが必要である。犯罪等の防止のため、いかに優れた暗号技術が開発されても、企業等が暗号技術を利用することの必要性を認識し、自ら利用しない限り、犯罪等の防止の効果は極めて限定されたものにならざるを得ない。

しかしながら、企業等の情報セキュリティ意識に関する現状は、多くの企業が情報セキュリティ対策に不安を感じてはいるものの、その不安が必ずしも対策に結びついていない、あるいは、そもそも情報セキュリティに対する不安すら感じていない状況にあり、情報セキュリティに関する意識及びネットワークに係る不正行為に対する危機感が欠如している状況にある。

したがって、企業等の情報セキュリティ意識を高め、暗号技術を利用することの必要性を認識させ、企業等における盗聴、「なりすまし」等のネットワークに係る不正行為に十分対応できる情報セキュリティ対策を促進するためには、企業等に対して効果的な広報啓発活動を行うことが必要不可欠であると考えられる。

（イ）　効果的な広報啓発活動の在り方

効果的な広報啓発活動を行うためには、企業等内の職責に応じた内容、方法等により行うことが適切であり、経営者（役員）、情報システム管理者及び一般社員に分けて検討することが適切と考えられる。

a　すべての対象に共通の内容

すべての対象に共通の広報啓発の内容としては、次のようなことが考えられる。

(a) 犯罪等の実態

企業等がその事業に係る犯罪等を防止するための対策を講ずるためには、対策を講ずることの必要性を認識するとともに、効果的な対策を講ずるために必要となる犯罪等の発生状況やその手口等の犯罪等の実態についての情報を入手することが必要となるので、これらの情報を提供する。

政府等に対する情報セキュリティに関する要望事項の中でも、「各

種情報の開示・被害事例の紹介、啓蒙」、「不正が行われた場合の速やかな開示」等、犯罪等による被害の事例に関する情報提供を求める意見は多い（第２章５（２）参照）。

(b) ＩＤ、パスワード及び暗号鍵の適正な管理等

ＩＤ、パスワード、暗号鍵等ネットワーク上で個人識別のために利用される情報は、不正アクセスや暗号技術の不正利用等を可能にするものであり、これらが犯罪者等に不正に入手されることのないよう適正に設定及び管理される必要がある。第２章２（２）アの調査結果からは、現状のセキュリティ対策の成否がＩＤ、パスワードの設定及び管理の適否にかかっている状況が認められるが、既に述べたとおり、企業等の情報セキュリティに対する意識は低調であることから、ＩＤ、パスワードの設定及び管理が適正になされているとは考えられず、実際にネットワークを利用する一般社員に対して、ＩＤ、パスワード等の適正な設定及び管理方策その他ネットワークの利用に当たり留意すべき事項の周知徹底を行うとともに、情報システムの管理者に対しても犯罪実態等を踏まえた適切なＩＤ、パスワード等の管理措置の実施を促す必要がある。

(c) 犯罪等の被害を受けた場合における対処方法

企業等が被害を受けた場合においては、被害の拡大及び新たな被害の発生を防止するとともに、爾後、効果的な対策を講じていくためには、関係機関等が被害の事実及びその状況を早急かつ的確に把握することが必要であり、被害を受けた場合の届出先及び届出を行う際に把握しておくべき被害状況等の届出事項についてあらかじめ明確に企業等に知らしめておく必要がある。

(d) 優良な暗号技術の利用

ネットワークに係る犯罪等を防止するためには、暗号技術を用いることが必要であるが、効果的に暗号技術を利用するためには、暗号技術を利用する目的等に応じて適切な暗号技術を選択し、利用することが必要であり、これを可能とするために、暗号技術利用の必要性及び優良な暗号技術の紹介を行うことが必要であると考えられる。