演習　情報漏えいに関する対策

平成17年度 問3

問　情報漏えいに関する対策について

情報システムの利用範囲が広くなるにつれて，情報システムで取り扱う情報の中に，個人情報や企業の機密情報が多く含まれるようになってきている。このような情報が社外に漏えいすると，企業の存続にもかかわる大きな問題になる可能性がある。

システム管理エンジニアには，このような機密性の高い情報に対して，システムの物理面，管理面及び技術面から漏えいを防止するための対策と，漏えいした場合の損害を最小限に食い止めるための対策の検討が求められる。

情報漏えいに関する対策を検討する際には，関係部門とともに，機密性の高い情報を特定し，その漏えいリスクを明確にする必要がある。

その上で，漏えいを防止するために，物理面からは，入退室者の厳格な本人確認や外部記憶媒体の持込み・持出し制限などを検討する。管理面からは，相互チェックの仕組みやアクセス権限の適切な更新などを検討する。また，技術面からは，アクセス範囲の限定や外部記憶媒体への情報書込み制限の仕組みなどを検討する。

漏えいした場合の損害を最小限に食い止めるには，漏えいの事実を早期に把握して，迅速に対応することが求められる。そのためには，情報システムへのアクセスログの継続的な取得及びその評価の仕組み，関係部門と連携した漏えい時の対応体制や対応プロセスなどの確立が重要である。

あなたの経験に基づいて，設問ア～ウに従って論述せよ。

設問ア　あなたが携わった情報システムの概要と，機密性の高い情報の概要及びその情報が漏えいした場合の影響について，800字以内で述べよ。

設問イ　設問アで述べた情報について，関係部門と協力してどのような方法で漏えいリスクを明確にしたか。その上で，漏えいを防止するための対策，及び漏えいした場合の損害を最小限に食い止めるため講じた対策について，工夫した点を中心に，具体的に述べよ。

設問ウ　設問イで述べた対策について，どのように評価しているか。今後の課題は何か。それぞれ簡潔に述べよ。

論文構成（下書き）の例

筆者が作成した論文構成（下書き）例である。問題を見ただけでは，論文が書けそうにない人は，これを参考にして本文を展開してみよう。

論文構成の作成手順の詳細は「3.2　論文作成のテクニック」を参照してほしい。

設問**ア**

1．プロジェクトの概要
　C社は，チケット予約システムを運用
　A社から派遣社員を受け入れ
　データのバックアップ・保管・廃棄業務をD社に委託
2．機密性の高い情報の概要
　保有するデータには，住所・氏名・電話番号などの個人情報（顧客データ）あり
　顧客データはセンタシステムで一元管理，また，D社の遠隔地倉庫に移動させ保管
3．情報が漏えいした場合の影響
　何のチケットを購入したか他人に明かしたくない購入者が多い
　インターネット販売による場合は，郵送のため住所等の顧客データを入力
　顧客データが社外に漏えいした場合，大きな問題に発展

設問イ

1．機密管理の意義
2．漏えいリスクの明確化
　営業部門，情報システム部門，その他すべての部門の代表者が参集し，漏えいリスクを協議
　次の三つの漏えいリスクに特定
　①センタシステムからの漏えい
　②D社の遠隔地倉庫からの漏えい
　③各営業店舗がダウンロードして漏えい
3．漏えいを防止するための対策
　物理面，管理面，技術面に分けて，検討
　C社の情報セキュリティポリシに反映
　3.1 物理面の対策
　　IDカードを配布し，IDカードがなければ入退室不可
　　IDカードの有効期限は1か月
　　A社の派遣社員もC社要員と同じ取扱い
　　サーバ室への外部記憶媒体の持込みは，事前申請許可を得た者のみ

３．２ 管理面の対策
　D社の遠隔地倉庫では，C社要員が立会い，記録簿記入
　パスワード有効期間を半年とし，それを越えるとパスワードを変更させる
３．３ 技術面の対策
　各営業店舗がダウンロードできる顧客データの項目は，個人を特定できないもののみ
　センタシステムの顧客情報は，本番用プログラムのみが参照・更新可
４．漏えい時の損害を最小限にするための対策
継続的なアクセスログの取得
ログ解析ツールを利用して，不正アクセスがないかの定期的な評価
緊急時対応計画の策定，関係部門との緊密な連携

設問ウ

１．設問イの評価
１．１ サーバ室の入退室管理
　権限がないD社要員が，サーバ室に入室する事例
１．２ パスワードの変更
　更新するパスワードが簡単すぎたり，名前から容易に想像できる
　二つのパスワードを半年ごとに交互に使用
２．今後の課題
２．１ サーバ室の入退室管理
　C社要員がバックアップ媒体をサーバ室外まで移動
２．２ パスワードの変更
　悪いパスワード例を一覧表にまとめ，各要員に配布
　同じパスワードを再登録できない仕組みに変更
　セキュリティ研修でも強調

解答例

前ページの論文構成に基づいて筆者が作成した解答例である。この中から，キーフレーズ（書けそうな文章例）を抽出して，自分の論文に取り込んでいけばよい。

設問ア

数字を入れる。

自分の立場を明示する。

何度も同じ長い名称を書きたくない場合は，このようにカッコ付で略称を定義する。

数字を入れる。

設問イの伏線を書いておく。

漏えい時の影響の大きさを訴える。

1．プロジェクトの概要

C社は，国内外旅行などの各種チケット商品の予約受付業務や発券業務をオンライン処理するチケット予約システム（以下，当システムという）を運用している。当システムは，全国100か所の営業店舗に設置した800台の端末がネットワークを介してセンタシステムに接続されている。私は，C社のシステム管理エンジニアであり，当システムの運用責任者でもある。C社は，当システムの運用について，A社から派遣社員を受け入れており，また，データのバックアップ・保管・廃棄業務をD社に委託している。

2．機密性の高い情報の概要

当システムは，不特定多数の顧客を対象に運用されており，保有するデータの中に，住所・氏名・電話番号などの個人情報（以下，顧客データという）を含んでいる。顧客データの数は，累積で約200万人分程度あり，件数の点でも大量になっている。顧客データは，センタシステムで一元管理し，営業店舗サーバには格納していない。また，センタシステムでは，週に一度のフルバックアップと，夜間バッチ終了後の差分バックアップを毎日行い，D社の遠隔地倉庫に移動させ，保管している。

3．情報が漏えいした場合の影響

チケットの大半は，コンサートや演劇などに関するものであるが，中には，宗教問題等の複雑な利害関係を対象とするものもある。何のチケットを購入したか他人に明かしたくない購入者も多く，できるだけ店舗での販売にしているが，インターネット販売による場合は，郵送のため住所等の顧客データを入力させている。そこで，万一，その顧客データが社外に漏えいした場合には，購入者から苦情が殺到することが予想され，C社の存続にもかかわる大きな問題になりえると考えられた。

設問イ

1．機密管理の意義

機密性の高い情報には，システムの物理面，管理面及び技術面から漏えいを防止するための対策と，漏えいした場合の損害を最小限に食い止めるための対策の検討が求められる。

2．漏えいリスクの明確化

私は，情報漏えいに関する対策を検討する際には，関係部門とともに，機密性の高い情報を特定し，その漏えいリスクを明確にする必要があると考えた。そこで，営業部門，情報システム部門，その他顧客データに関与するすべての部門の代表者が参集し，漏えいリスクを協議した上で，次の三つの漏えいリスクに特定した。①情報システム部が管理しているセンタシステムから漏えいする。②D社の遠隔地倉庫で保管しているバックアップから，もしくは破棄する時に漏えいする。③各営業店舗が販売分析用にセンタシステムからサーバにダウンロードしている顧客データが漏えいする。

3．漏えいを防止するための対策

私は，漏えいを防止するための対策を，物理面，管理面，技術面に分けて，それぞれ検討した。その主なものは，次のとおりであり，これらをすべてC社の情報セキュリティポリシに反映させた。

3．1　物理面の対策

顧客データが格納されているセンタシステムのサーバ室への入退室者の厳密な本人確認を実施するために，IDカードを各要員に1枚ずつ配布した。IDカードがなければ入退室ができず，入退室情報をログとして記録した。IDカードの有効期限を1か月とし，1か月ごとに更新する手続を組み込んだ。A社の派遣社員もC社要員と同じ取扱いとした。

また，サーバ室への外部記憶媒体の持込み，もしくは持出しを制限し，事前申請許可を得た者に限定した。

問題文をそのまま，引用する。

問題文をそのまま，引用する。

設問アで定義した略称を使用する。

「漏えいする」という表現が，くどい気もするが，そのまま流れに乗って書き続ける。

キーワードを書いて，専門的な知識を知っていることをアピールする。

一般的な対応策を書く。

一般的ではない対応策も書いてみる。

立会いと記録簿作成は，対応策の定番であるので，覚えておく。

パスワードの有効期間設定は，対応策の定番であるので，覚えておく。

思いつきにくい対応策であるが，論文に変化をつけるために書いてみた。

問題文の趣旨を引用し，当システムに適用した文を書く。

キーワードを書いて，専門的な知識を持っていることをアピールする。

3．2　管理面の対策

　D社の遠隔地倉庫でバックアップを保管する場合の顧客データの持出し時には，C社要員が必ず立会い，記録簿に記入させた。この手続は，データを廃却する時に，遠隔地倉庫から焼却所に移動させる場合も同様とし，顧客データを格納している媒体を焼却炉に投入する所まで確認させた。

　また，A社の派遣社員を含む当システムにアクセスする者全員に，IDとパスワードを個人ごとに与え，管理している。そのパスワード有効期間を半年とし，有効期間を越えると，パスワードを変更させる仕組みを採用した。

3．3　技術面の対策

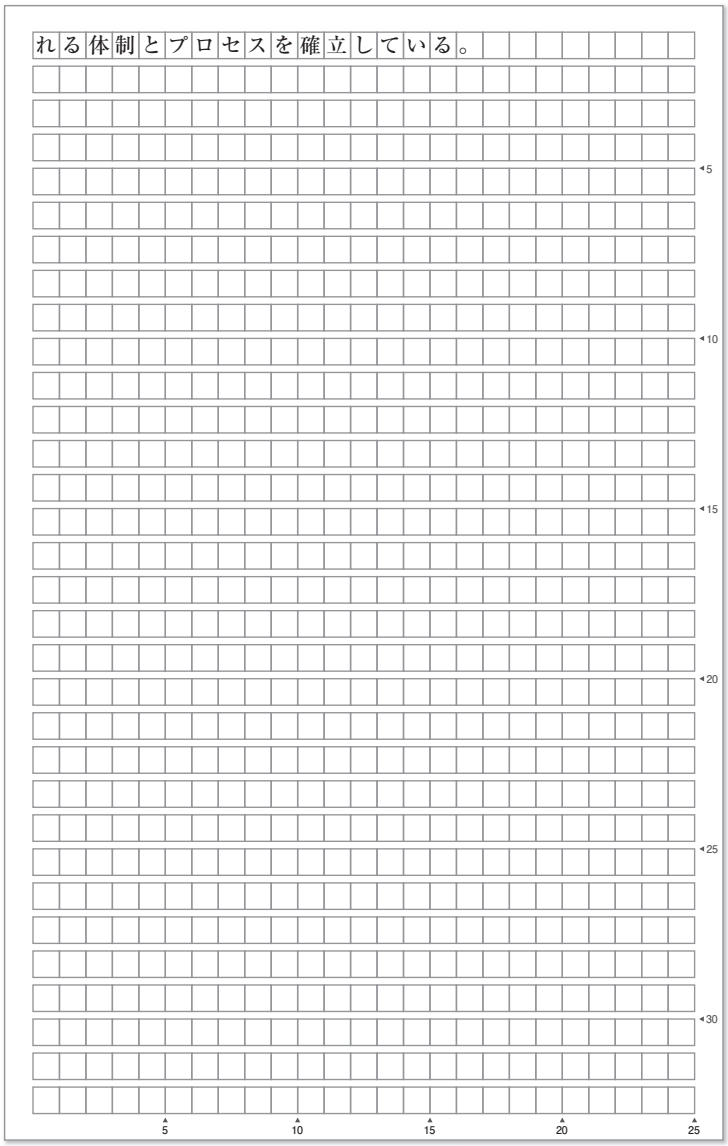
　各営業店舗が販売分析用にセンタシステムからサーバにダウンロードしている顧客データには，住所や氏名などの詳細な個人情報は不要であると結論づけた。そこで，ダウンロードできる顧客データの項目は，性別や年齢帯などの個人を特定できないもののみとし，アクセス範囲を限定した。

　また，センタシステムのサーバに格納されている顧客情報は，本番用プログラムのみが参照・更新可能とし，ユーティリティを利用してMO等の外部記憶媒体へ書き込むことを不可能にした。

4．漏えい時の損害を最小限にするための対策

　私は，漏えい時の損害を最小限にするためには，漏えいの事実を早期に把握して，迅速に対応することが重要と考えた。そのため，センタシステムに格納しているデータのすべてについて，継続的にアクセスログを取得している。取得したアクセスログは，ログ解析ツールを利用して，不正アクセスがないかを定期的に評価している。

　また，万一，情報漏えいが発生した場合を想定して，緊急時対応計画を策定し，関係部門との緊密な連携が取



設問ウ

決まり文句を入れる。

失敗した点をハッキリと示す。

改善策をハッキリと示す。

改善策をハッキリと示す。

言い足りないことかあれば，「また」でつないで，追加する。

1．設問イの評価

　私が実施した情報漏えいに関する対策は，おおむね良好に機能したと評価している。現時点では，顧客データを含む情報漏えいは，発生していない。ただし，以下の点は改善する余地を残していると考えている。

1．1　サーバ室の入退室管理

　D社の遠隔地倉庫へバックアップを搬送する時に，IDカードを持たないD社の要員に，自分のIDカードを渡し作業をさせるC社要員がいた。すなわち，本来，権限がないD社要員が，サーバ室に入室する事例が数件あった。

1．2　パスワードの変更

　半年ごとに更新するパスワードが，要員によっては簡単すぎたり，名前から容易に想像できるものであるケースが散見された。また，二つのパスワードを半年ごとに交互に使用する者もいた。

2．今後の課題

2．1　サーバ室の入退室管理

　バックアップ媒体は，C社要員が自分のIDカードを使って，サーバ室外まで移動することを徹底させる。D社には，バックアップ媒体の受渡し場所は，サーバ室前である点を書面にて報告し，D社要員にもその旨を周知させる依頼を行う。

2．2　パスワードの変更

　悪いパスワード例を一覧表にまとめ，各要員に配布する。同一人が過去に入力したパスワードを記録し，同じパスワードを再登録できない仕組みに変更する。また，これらの点は，定期的に実施しているセキュリティ研修でも強調するようにインストラクタに指示する。