IPA®
INFORMATION-TECHNOLOGY PROMOTION AGENCY, JAPAN

情報化月間2007記念式典特別行事
情報漏えい対策セッション
＜パネルディスカッション＞
2007年10月1日

現状での一般的な情報漏えい対策

独立行政法人 情報処理推進機構
セキュリティセンター
ウイルス・不正アクセス対策G
研究員　木邑 実

情報セキュリティマネジメント

（1）守るべき情報資産は何か？
（2）どのような脅威があるか？
（3）被害の想定
（4）対策案の検討
（5）セキュリティポリシーの策定
（6）対策の徹底
（7）対策状況の確認
（8）対策の見直し

■情報資産の洗い出し

- 何があるか？

  電子ファイル、紙、コンピュータ、ネットワーク、．．．

- 利用目的は？
- 誰が使うのか？
- どこにあるのか？
- いつ使うのか？

情報資産管理台帳の作成

情報の分類と格付け（機密性、完全性、可用性）

■情報漏えいの脅威

- 紛失・盗難
- 誤送信・誤公開
- 従業員による不正持ち出し
- ウイルス等の不正プログラムによる送信・公開
- Winny等のファイル交換ソフトからの流出
- 外部からの不正アクセスによる情報参照
- 風評・ブログ掲載

■被害の想定と対策案の検討

- 個人情報流出 => 信用失墜 => 顧客離れ
- 銀行口座番号・クレジットカード情報・IDパスワード等の流出 => 預金盗難、不正利用、架空請求等 => 金銭的被害 => 損害賠償請求
- 機密情報流出
- 営業活動制限 => 機会喪失 => 売り上げ減少
- 対応費用発生 => 利益減少

■情報漏えい対策（例）

技術的対策

- アクセス制限
- 暗号化
- ウイルス対策
- ネットワーク接続制限

物理的対策

- 入退室管理
- 鍵付き収納庫
- シュレッダー機器
- シンクライアントPC

人的・組織的対策

- 運用ルール
  - ・PC持出制限
  - ・情報廃棄
- 教育
- 契約
- アクセスログ
- 監査
- 保険
- インシデント対応マニュアル

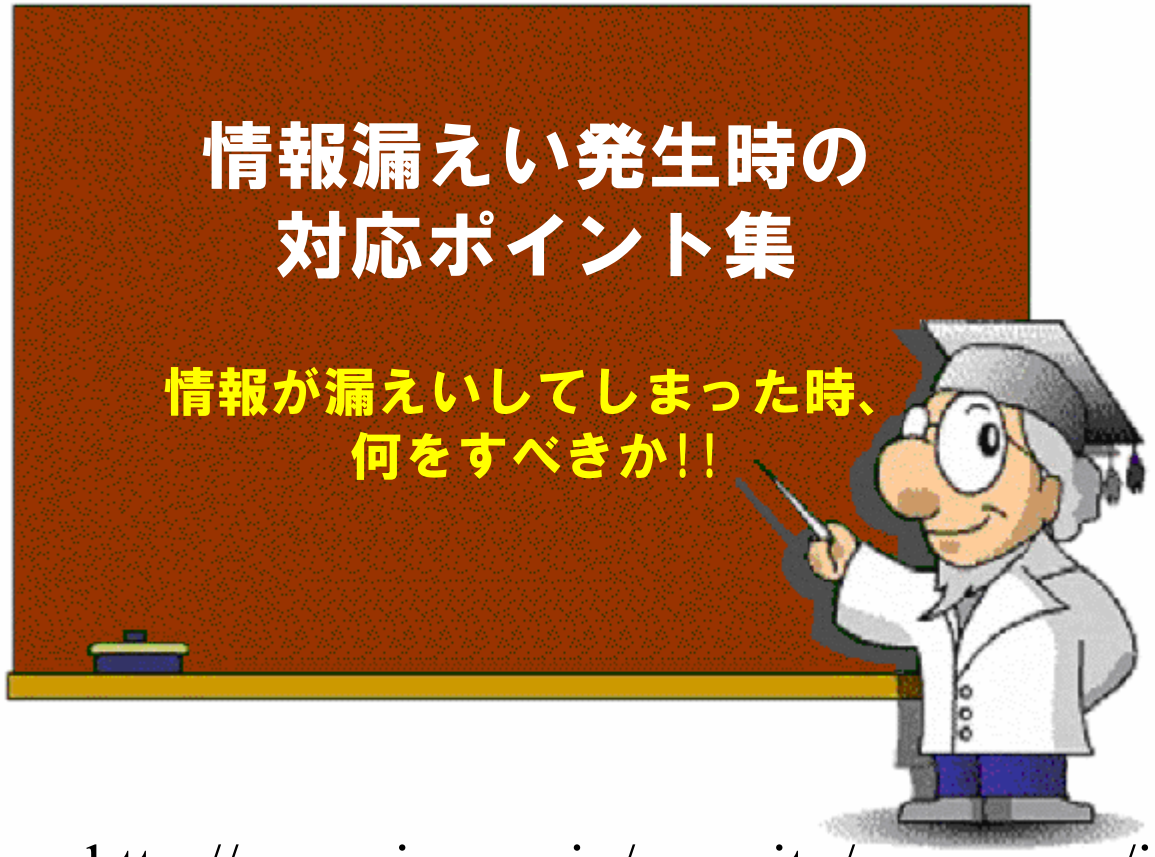
■情報漏えい対策例（もう少し具体的に）

- 使う人だけにアクセス権限を付与
- 強固なパスワード設定ポリシ
- 指紋などのバイオメトリックス認証の活用
- スクリーンセーバのパスワードロック設定
- 最新のウイルス定義情報で常時監視・定期的な全スキャン
- 不要なサービスの停止
- USB端子への接続制限
- 同報メール送信専用システムの導入
- ハードディスク丸々暗号化

■情報漏えい対策例（もう少し具体的に）

- 人事異動にリンクしたID管理
- PCや情報の持ち出しルールに例外条件と手続きを明記
- 例外処理の承認ルール及びチェック体制
- 専用ソフトによる廃棄・返却パソコンのディスク完全初期化
- 具体的な脅威や被害を教育で教える
- 請負契約審査時、セキュリティ対策が充分かチェック
- メール、ウェブアクセス、ソフトインストールのログをとるシステムの導入と従業員への説明
- インシデント対応マニュアルによる予行演習

情報漏えい発生時の対応



http://www.ipa.go.jp/security/awareness/johorouei/

情報漏えいインシデント対応方策に関する調査 報告書
http://www.ipa.go.jp/security/awareness/johorouei/index2.html

１　基本的な考え方

情報漏えい対応の目的

「情報漏えいによる直接的・間接的被害を最小限に抑える」

情報漏えい対応の５原則

（１）被害拡大防止・二次被害防止・再発防止の原則

（２）事実確認と情報の一元管理の原則

（３）透明性・開示の原則

（４）チームワークの原則

（５）備えあれば憂いなしの原則

２　情報漏えい対応の基本ステップ

情報漏えい発生！

（1）
発見・報告

速やかに責任者に報告し対応のための体制を構築
不用意な操作を避ける
外部からの通報は、相手の連絡先を控える

（2）
初動対応

対策本部を設置
被害の拡大、二次被害の防止のための応急処置
（情報の隔離、ネットワークの遮断、サービスの停止など）

（3）
調査

5W1H（いつ、どこで、誰が、何を、なぜ、どうしたのか）で調査し情報を整理
重要な情報に関する証拠を確保

（4）
通知・報告・公表
等

個人情報の本人、取引先などへの通知
監督官庁への報告、警察、IPAなどへの届出
ホームページ、マスコミ等による公表を検討

（5）
抑制措置と復旧

被害の拡大の防止と復旧措置
再発防止に向けた取組み

（6）
事後対応

抜本的な再発防止策を実施
被害者に対する損害の補償
内部職員の処分
最終的な情報開示

３　情報漏えいのタイプ別対応ポイント

（１）情報のタイプとポイント

個人情報	**顧客等、個人に関する情報** **個人情報保護法に準拠した対応が必要（監督官庁へ報告）** **本人への通知や注意喚起など被害防止措置が必要**
公共性の高い情報	**社会の重要なサービス、安全に関する情報など** **関係者・監督官庁への報告** **マスコミ等へ情報を開示**
一般情報	**取引先等の情報については取引先に連絡** **情報の当事者の意向に沿った対応を実施** **組織の重要情報については内容に応じた経営判断を実施**

（2）漏えいのタイプとポイント

	（1）発見・報告	（2）初動対応	（3）調査	（4）通知・報告・公表等	（5）抑制措置と復旧	（6）事後対応
（1）紛失・盗難	製造番号等固有の特徴情報があると発見しやすい	アカウントの停止・パスワードの変更	情報の内容を特定 中古・オークション市場を調査	本人への通知と謝罪		
（2）誤送信・Webでの誤公開等		送付先への削除依頼	流出先・内容の特定	公表・謝罪	相談窓口の開設 ユーザ教育	
（3）内部犯行	通報者の連絡先確認	警察への相談 証拠の確保	漏えい 情報とアクセス可能なユーザの特定		情報管理体制の強化	
（4）Winny/Share等への漏えい	通報者の連絡先確認	漏えい元の調査 Winny利用の停止	漏洩情報の確認	公表は被害拡大がないことを確認の上	事態の鎮静化	
（5）不正プログラム	通報者の連絡先確認		漏洩情報および流出先の確認	被害状況の報告・公表		
（6）不正アクセス	通報者の連絡先確認	警察への相談 証拠の確保	漏洩情報および流出先の確認	被害状況の報告・公表		
（7）風評・ブログ掲載等		掲載者への連絡と削除通知	従業員が勝手に反応しないよう指導		事態の沈静化	

表だって反応しない

4　発見・報告について

不確かでも迅速な第一報を責任者に
5W1Hで情報を整理
被害拡大・二次被害防止の観点から応急処置

発見報告用情報共有シートの例

件名	○○の情報漏えいについて		
報告者所属	○○事業部○○担当	発災当事者所属	○○事業部○○担当
報告者氏名	情報　太郎	発災当事者氏名	漏洩　次郎
報告者Tel	03-XXXX-XXXX	発災当事者Tel	03-XXXX-XXXX
報告者Mail	XXX@XX.XX	発災当事者Mail	XXX@XX.XX
下記の事項で、判明していることを記述する。 初報なので、不明な項目は不明として迅速に報告する事。			
◆情報漏洩の情報のソース（誰が発見したのか、どこから漏洩情報を入手したのか）			
◆情報漏洩判明日時			
◆情報漏洩発生日時			
◆情報漏洩内容			
◆情報漏洩内容の件数			
◆想定される原因			
◆対応状況（行なっていれば記述） ・特に組織外からの通報の場合、相手が何を要求しているのかを記述			

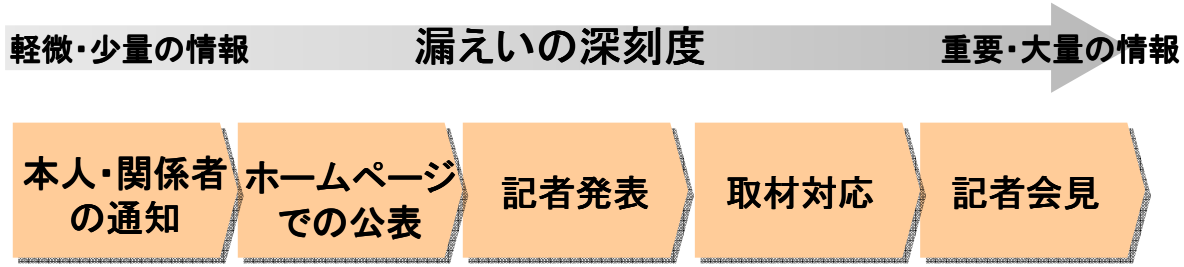
５　通知・報告・公表等について

通知・報告・公表の目的

「情報漏えいによる直接的・間接的被害を最小限に抑える」

本人・関係者に漏えいの事実を伝え二次災害防止のための注意喚起を行う。

重要



✓正確な情報を伝える

✓組織としての統一見解を整理し内容がぶれないように窓口を一本化

✓取材が多い場合は記者会見を実施

参考. 公表用資料に含むべき項目(例)

序文(発生した情報漏えいに関する謝罪、会社としての姿勢など)

事故発生に関する状況報告

事実経緯

調査方法及び状況

漏えいした情報の内容

事故の被害内容(二次被害の影響含む)

事故原因

当面の対応策

再発防止策

問い合わせ窓口(事故に関する連絡先)