

# ソフトバンクBB 情報セキュリティへの取り組み

ソフトバンクBB株式会社  
情報セキュリティ・品質管理本部  
本部長 高 元伸

2005年7月8日



# アジェンダ



- 情報セキュリティの目的
- セキュリティ事故と情勢
- ソフトバンクBBの情報セキュリティ対策
- 情報セキュリティ事故を防ぐには

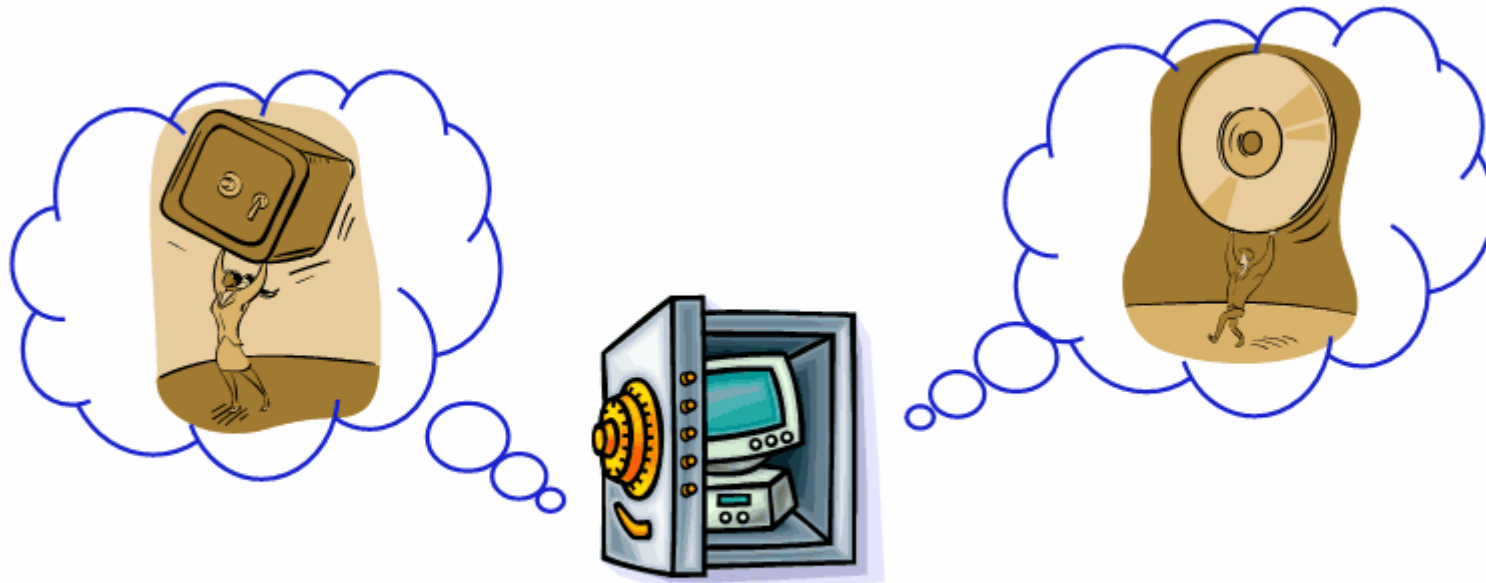


# 情報セキュリティの目的

# 情報セキュリティの目的

SoftBank BB

情報は利用してこそ価値がある



正しく管理してこそ安心がある

# 情報資産

- **経営情報**
  - 組織運営上に影響する情報。財務諸表、取締役会議事録等
- **業務情報**
  - 業務を遂行する上で必要な情報。業務マニュアル、品質管理マニュアル、文書管理マニュアル等。営業情報(企業情報)
  - 営業活動上必要な企業情報。顧客企業の情報、競合企業の情報等
- **技術情報**
  - 社内固有の技術情報。NW構成図、機器仕様詳細、製品ロードマップ等
- **営業情報(個人情報)**
  - 営業活動上必要な個人情報。顧客の個人情報、潜在顧客の個人情報等
- **マーケティング情報**
  - 営業情報等から加工したマーケティング活動を目的とした情報
  - 最終的には、市場に公開することを目的としている

# セキュリティリスクの例

- ウイルスによってOSが破壊された。
- 帰宅途中にPCを紛失した。
- スпамメールによってシステムが一日利用できなくなった。
- ハッキングにあってホームページが書き換えられた。
- 故障によりシステムが停止し、重要取引が1週間延期された。
- 新規サービスの企画書が盗まれた。
- 顧客リストが社外に漏洩した。

# セキュリティ事故による影響

- 代替処理・回復処理等の余分な業務処理の業務量
- 信頼回復のためのコスト
- 損害賠償のコストや訴訟コスト
- 信用失墜による(既存および潜在的)顧客の喪失による損失
- 売上機会の損失
- 当局等に対する対応、制裁
- 二次被害
  - 事務処理等のミスによる損失
  - マスコミや顧客への対応ミスによる更なる信用の損失

**情報セキュリティは企業の社会的責任**

# 情報セキュリティ事故と情勢



# ソフトバンクBBにおける情報流出事件



03年9月: Pマーク取得の為に、個人情報保護管理委員会発足

03年10月: 情報資産の洗い出し活動を展開

04年1月: ISMS認証基準に基づいたリスクアセスメント実施

04年2月 情報漏えい報道

## K事件

2004年1月 業務委託として、ソフトバンクBBに従事していたKが、  
顧客情報を持ち出し、1,000万円を要求

2004年2月 逮捕

2004年3月 起訴

2004年7月 有罪判決(恐喝未遂)確定

## Y事件

2004年1月 顧客情報が不当に入手され、Yが外部のものと共謀の上  
20億～30億円と、月に数百万円を要求

2004年2月 逮捕

2004年3月 起訴

2004年8月 有罪判決(恐喝未遂)確定

その他4名が事件に関連して逮捕・起訴

(不正アクセス行為の禁止等に関する法律違反、恐喝未遂幫助、等)

# 情報漏えいによる影響

SoftBank BB



出展: gooリサーチ:04/06/09

- 顧客へのお詫び
- メディアへの取組告知
- 信頼喪失による顧客の解約
- 潜在的ビジネス機会のロス
- 信頼回復の対策費用 (設備投資・運用コスト)

経営に対する重大な影響

# 市場での最近の情報漏えい事故

## 管理規定外の場所での流出

- 米国において約4000万枚のクレジットカード顧客情報が流出
  - 提携の情報処理会社が規定に反してデータを保持
- 総合電気会社の子会社からWinny(ウィニー)により発電所20ヶ所の情報が流出
  - 子会社社員が自宅へデータを持ち出しで
- 愛知県警にてWinny(ウィニー)により捜査情報が流出
  - 巡査が職場で私物PCを使用し自宅でネットワーク接続時

## 社外持ち出しPC

- 紛失・置き忘れ・盗難・車上荒らし・空き巣
  - 業界・件数・内容を問わず日常的に発生

# PCの盗難・メール誤送信



## 個人情報漏洩事件一覧

- 2005/04/26 [近鉄百貨店、アクセサリ売り場の顧客リストが盗難](#)
- 2005/04/26 [NTTデータ、NTT西日本の顧客情報2146件を保存したPCが盗難被害に](#)
- 2005/04/25 [日本郵船、採用試験受験者122名分の履歴書を紛失](#)
- 2005/04/25 [北陸ガス、顧客情報31件分が記載された領収書綴りを紛失](#)
- 2005/04/25 [ミニストップ、紛失した収納票控を回収](#)
- 2005/04/22 [みちのく銀行、顧客情報131万件を紛失](#)
- 2005/04/22 [北陸銀行子会社、個人情報に記載された振込依頼書などを誤送付](#)
- 2005/04/22 [ちば興銀ユーシーカードが支払依頼書を他の顧客へ誤送付](#)
- 2005/04/21 [人材派遣業のフルキャスト、車上荒らして個人情報を紛失](#)
- 2005/04/21 [廃棄パソコンから生徒の個人情報が漏洩 - 静岡](#)
- 2005/04/20 [トヨタ、システム開発委託先から顧客情報が流出](#)
- 2005/04/19 [トヨタディーラー、個人情報入りパソコンが盗難被害](#)
- 2005/04/19 [佐賀銀行、誤送付により個人情報を流出](#)
- 2005/04/15 [湯沢市民の個人情報が流出 - P2ソフト経由のウイルス感染が原因](#)
- 2005/04/15 [福岡クボタ、6万件の個人情報入りパソコンが盗難](#)
- 2005/04/15 [認定個人情報保護団体が個人情報を漏洩 - メール送信ミスで](#)
- 2005/04/15 [JR北海道、定期券申込用紙を焼却処分 - 個人情報流出の可能性](#)
- 2005/04/15 [ジャスコ鳥取店、個人情報が記入された保険申込書を紛失](#)
- 2005/04/14 [多摩郵便局、個人情報が記載された配達業務監査用紙を紛失](#)
- 2005/04/14 [茨城銀行、FAX誤送信により顧客情報を流出](#)
- 2005/04/14 [市職員が個人情報を業者へ提供 - 千葉市](#)
- 2005/04/14 [二重の県立高校、PC盗難で生徒の個人情報が流出の可能性](#)

### NTTデータ、NTT西日本の顧客情報2146件を保存したPCが盗難被害に

NTTデータは、社員の自宅に空き巣が入り、NTT西日本の顧客情報2146件が保存されたノートパソコンが盗難に遭ったと発表した。

同社によれば、4月14日、社員の自宅に空き巣が入り、会社から貸与されたノートパソコンが盗難に遭った。同パソコンには、NTT西日本が扱うインターネット関連商品のデータベース整備作業に関わる顧客情報2146件が保存されており、氏名、住所、電話番号、メールアドレスなどの個人情報が含まれていた。警察に被害届を提出したが、現時点では発見されていない。

被害に遭った顧客に対しては、NTT西日本より個別にお詫びを行うとともに、電話での問い合わせにも応じるという。同社では、再発防止に向けて、個人情報の入ったパソコンの指定作業場所以外への持ち出し禁止、盗難発生時の対応マニュアルの整備などの強化を図るとしている。

### 総務省、メール誤送信によりモニター27名の個人情報を流出

お客様情報の入ったノートパソコンの総務省関東総合通信局は、メールの誤送信により、電気通信サービスモニター27名の個人情報を流出したと発表した。  
<http://www.nttdata.co.jp/release/>

総務省関東総合通信局は、メールの誤送信により、電気通信サービスモニター27名の個人情報を流出したと発表した。

NTTデータ  
<http://www.nttdata.co.jp/>

同局によれば、3月28日、電気通信サービスモニター27名に「メールアドレス登録確認メール」を送信した際、誤って、27名全員の氏名およびメールアドレスが表示される状態で送信したという。

(by IT保険ドットコム、2005/04/26)

同局では、ただちに事実説明とお詫びを行うとともに、誤送信されたメールの削除と、メールアドレスの変更を要請した。今後は、個人情報のさらなる厳重な管理に努めるとしている。

個人情報流失事故について  
<http://www.kanto-bt.go.jp/press/p16/p1703/p170329.html>

総務省関東総合通信局  
<http://www.kanto-bt.go.jp/>

(by IT保険ドットコム、2005/03/30更新)

出展:IT保険ドットコム(2005/04/2)

# 個人情報保護法による変化

## 事業者の義務

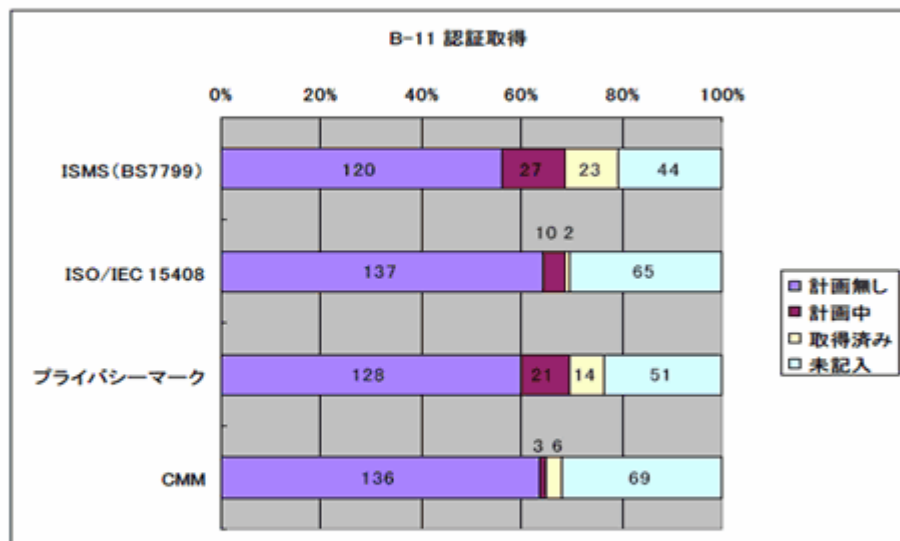
- 利用目的の特定・制限
- 適正な取得・利用目的の通知
- 正確性の確保
- 安全管理措置
- 第三者提供の制限
- 管理監督責任
- 開示・訂正・利用停止等
- 苦情の処理

## 消費者の権利

- 事業者が保有する個人データに関して、  
『本人が関与できる仕組み』
  - 開示
  - 訂正
  - 利用停止

# 企業の取り組み

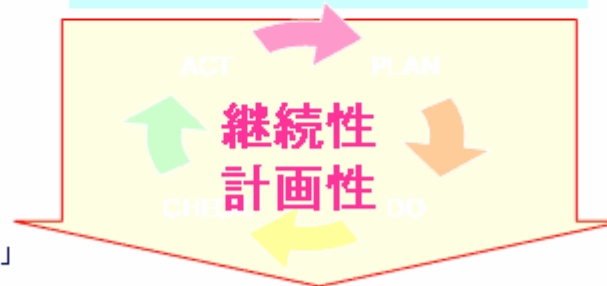
| 名称            | 計画無し |       | 計画中 |       | 取得済み |       | 未記入 |       |
|---------------|------|-------|-----|-------|------|-------|-----|-------|
| ISMS(BS7799)  | 120  | 56.1% | 27  | 12.6% | 23   | 10.7% | 44  | 20.6% |
| ISO/IEC 15408 | 137  | 64.0% | 10  | 4.7%  | 2    | 0.9%  | 65  | 30.4% |
| プライバシーマーク     | 128  | 59.8% | 21  | 9.8%  | 14   | 6.5%  | 51  | 23.8% |
| CMM           | 136  | 63.6% | 3   | 1.4%  | 6    | 2.8%  | 69  | 32.2% |



平成16年10月 NPO調べ「ITセキュリティ対策の導入状況と満足度に関する調査」  
n=416

情報セキュリティ監査  
の要求項目(経産省)

- ・基本方針
- ・組織のセキュリティ
- ・資産の分類
- ・人的セキュリティ
- ・物理的及び環境的セキュリティ
- ・通信及び運用管理手順
- ・アクセス制御
- ・システムの開発及び保守
- ・事業継続管理
- ・適合性(コンプライアンス)



セキュリティ関連認証を取得するには、計画・実行・監査・再計画のサイクルが必要となり、**継続的な見直し体制**が必要となる。

# 個人情報保護と活用

SoftBank BB

## 個人情報 (顧客情報・従業員情報)

### 活用

- ・ダイレクトマーケティング
- ・顧客情報を活用した新しいサービス
- ・CRM強化による顧客満足度の向上

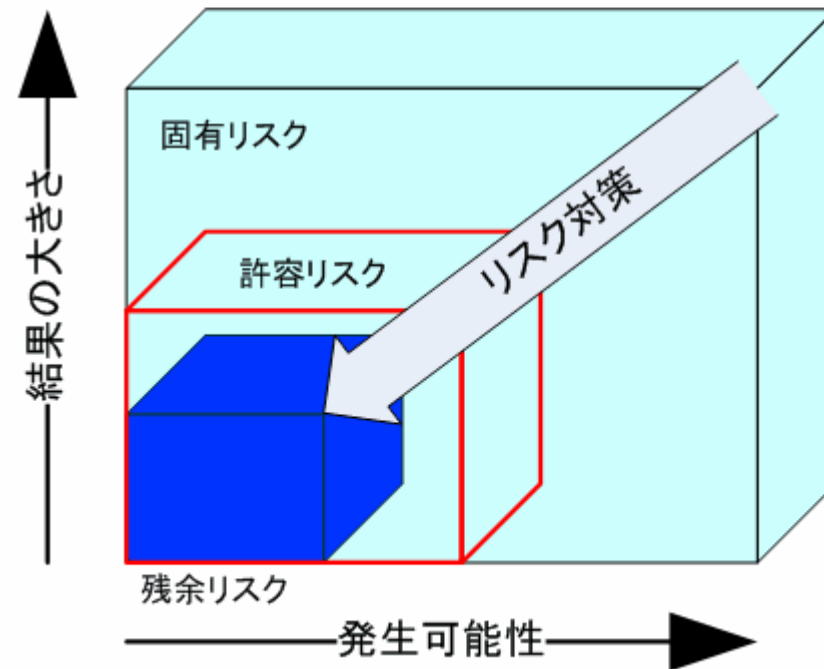
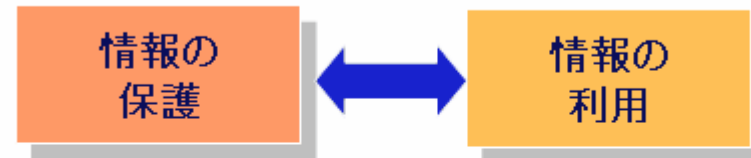


### リスク管理

- ・市場からの評価、企業価値
- ・業務プロセスに潜む脆弱性
- ・社員のモチベーション

# 対策の限界と残るリスク

- リスクマネジメント
  - 損失のエクスポージャー
  - 潜在的な利益
- 組織活動においての情報の意味
  - 利用しなければ意味がない
  - 必要だから情報を持っている
- 陥りやすいマネジメント手法
  - 保護するだけ
    - 機密性 確保
    - 完全性 確保(?)
    - 可用性 確保できていない

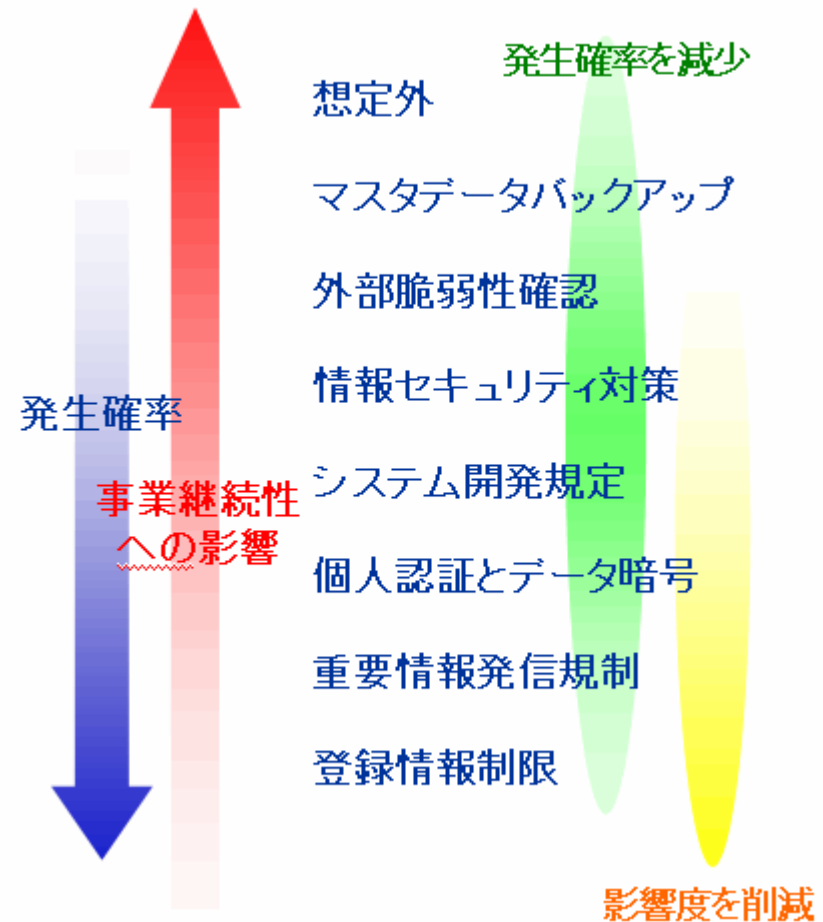




# 発生の可能性と対応

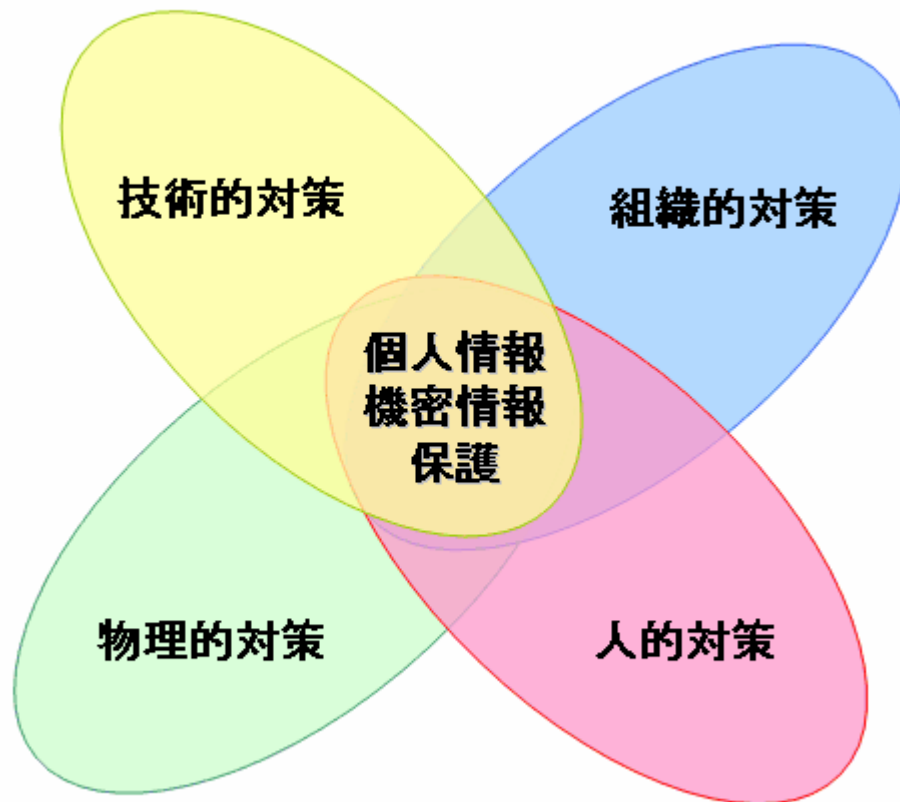
SoftBank BB

- 隕石が本社を直撃
- 直下型地震でIDCが倒壊
- 高度な犯罪集団によるハッキング
- 大規模顧客情報漏えい・不正使用
- システム誤作動による不適情報発信
- 重要情報の入ったPCの盗難
- FAX誤送信
- 携帯電話の紛失



# ソフトバンクBBの 情報セキュリティ対策

# 情報セキュリティ対策の基本方針



## 組織的対策

- CISOの任命
- 情報セキュリティ委員会の設置
- 各部門でセキュリティ担当を任命…

## 人的対策

- コンプライアンス教育の徹底
- 誓約書提出とルールの徹底
- 業務委託先との再契約…

## 物理的対策

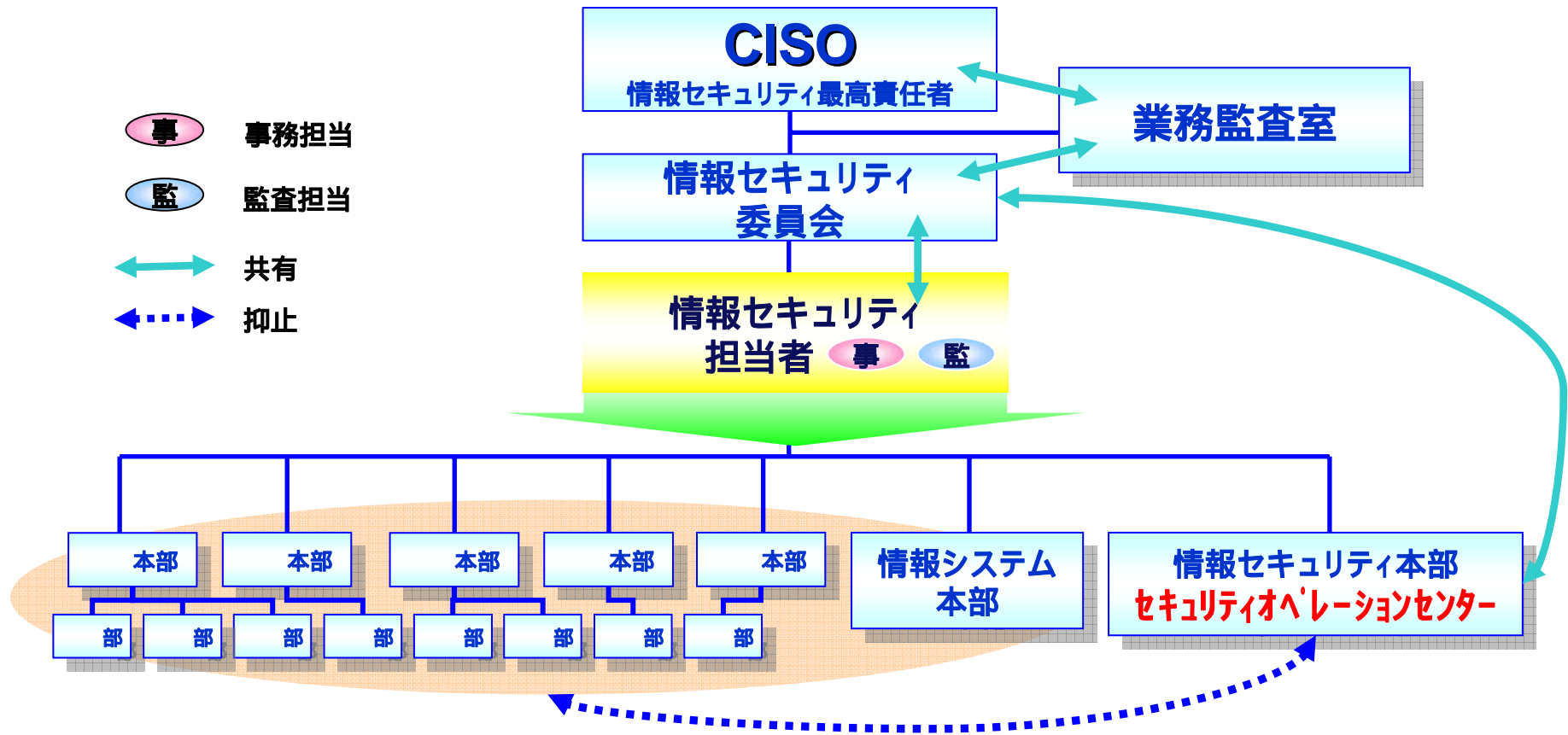
- 高セキュリティエリアの設置
- セキュリティゲートの設置
- 認証による入退室の制限…

## 技術的対策

- ログの収集・解析
- リアルタイム監視
- バイオ認証
- セキュリティPC…

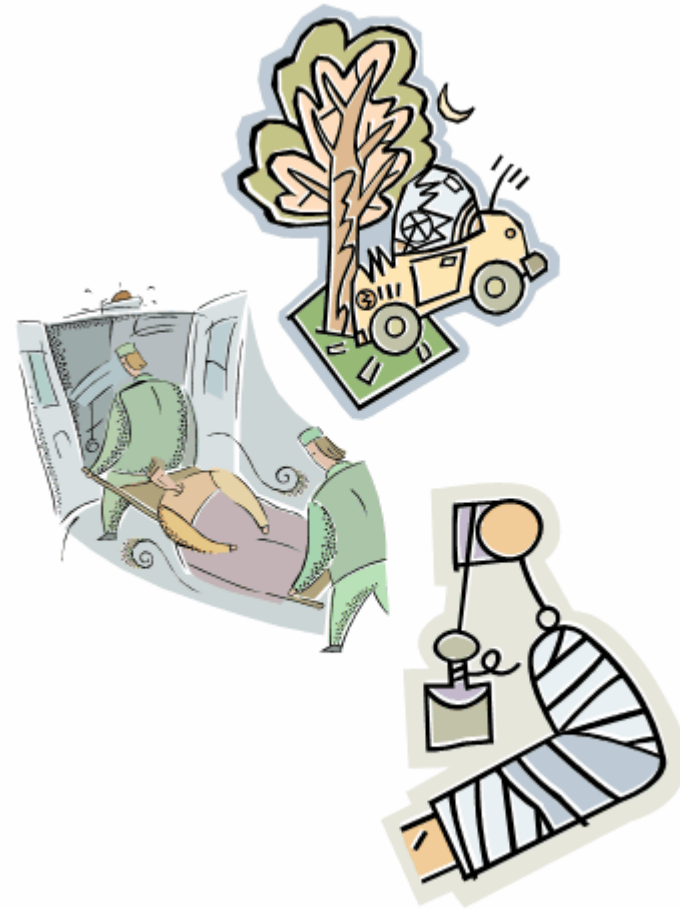


# 組織的対策



# 組織的対策 ～ 危機管理

- 想定されるリスクと対応体制の確認
  - PCの盗難・紛失
  - 個人情報目的外使用
  - 顧客リストの流失可能性問い合わせ
- 対応担当者の連携
  - 経営責任者
  - 情報セキュリティ責任者
  - 情報セキュリティ担当実務
  - 法務・コンプライアンス
  - 広報
- 被害を最小限に抑える
  - 迅速な情報提供
  - 被害範囲・内容・経路の確認
  - 二次災害防止
  - 再発防止



# 物理的対策 汐留本社

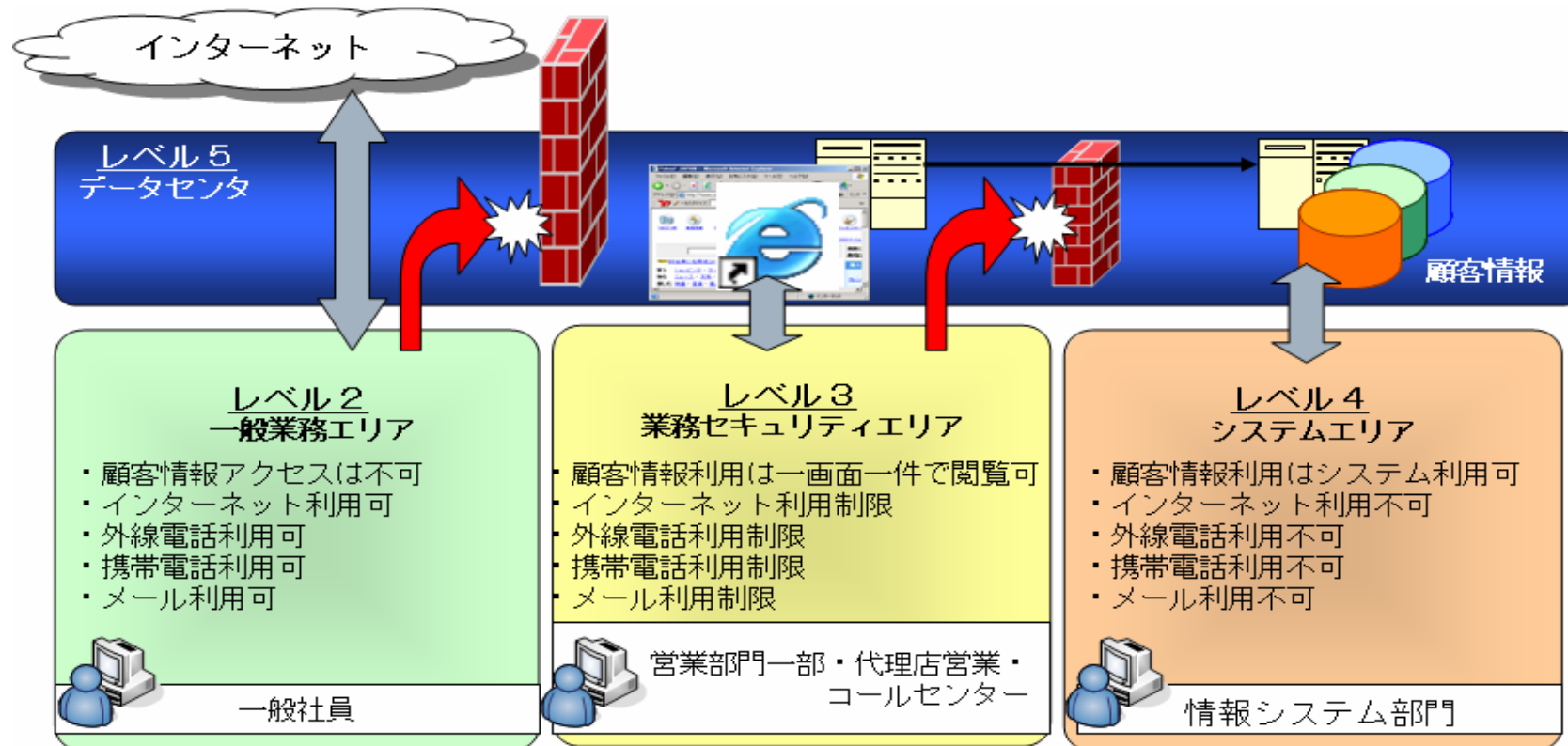


2005年2月 本社移転に伴い、ファシリティのセキュリティレベルを更に強化



# 物理的対策 ～セキュリティレベル

- ネットワークを分割し、顧客情報を物理的セキュリティ境界にて隔離
- 業務内容別作業エリアを設定し、システムやツールの制限を定義



# 技術的対策

- **入退出管理**  
ICカード・申請書および警備員確認による入出管理 24h・365Day 有人警備
- **監視カメラ(ビデオ)**  
エリア内での作業員の行動を映像で記録・保管
- **セキュリティゲートの設置**  
エリア内へのモバイル機器・携帯電話などの持ち込み持ち出し検査
- **バイOMETRICS(生体認証)の導入**  
バイオ認証(生体)登録者のみがPCを經由して限定・承認された作業のみ可能
- **外部記憶装置の制限**  
不要な外部記憶装置(FD、DVD-R等)が一切利用できないIPCの設置
- **監視ソフトの導入**  
PCの操作履歴を監視するソフトを導入 SOCによる常時監視
- **リアルタイム監視の実施(SOC 高セキュリティエリア内)**  
申請許可以外の外部メディア利用やデータ転送を監視





# 技術的対策 ～ 持ち出しPC

- **私用PCの業務利用は禁止**
  - 社内ネットワークに接続できない
  - 罰則対象
  - 検証目的利用であっても会社支給で検証用ネットワークのみ接続可能
- **業務エリア外からの持ち出しを原則禁止**
  - 出張時等は上長の承認が必要
  - 重要情報システムエリアへのリモートからの接続制限
  - 盗難紛失時のデータ閲覧を防御
    - BIOSパスワード - OSそのものが起動しない
    - 生体認証 - 本人でないと操作ができない
    - ディスク暗号化 - 物理的に分解されてもデータが参照できない
- **全ての操作ログの保持**
  - 会社資産および業務目的のみの使用
  - 紛失再発見時に不正使用の検証が可能

# 人的対策

- e-Learning・集合研修
- 業務に従事する者の知識・モラルの向上
- 業務委託契約の全面見直し
  - 個人からの誓約書
  - 企業との機密情報取り扱いに関する契約



# 人的対策 オリジナル e-Learning

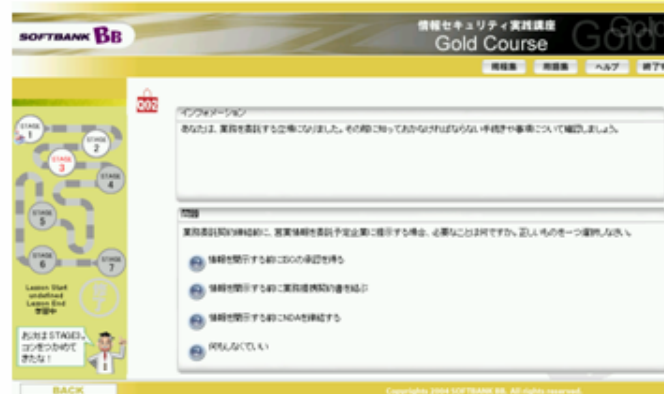
## ① 入門コース 【Bronze】



皆さん、こんにちは。CISOの阿多です。  
このコースをご覧になっている皆さんは、ソフトバンクBBのセキュリティ対策に関する取り組みについて、すでに学習を始めていただいていると思います。  
ご存知の通りソフトウェアは、常に新しいビジネスモデルに、変化を求められ続けています。一方、セキュリティ対策を重要視していることも皆さんに是非知っていただきたいです。  
セキュリティは一度きりの対策が終わるものではなく、永久に続けていくものです。

CISOである阿多さんからメッセージです。

## ③ 実践コース 【Gold】



インフラ担当者  
取組の上、業務を遂行する立場になります。その際においておこななければならない対策や準備について確認しましょう。

実践  
業務遂行の前提として、現実業務を前提とした実践を行う場合、必要なことは何か、正しいものを一つ選択してください。

- ① 情報を開示する前におこなう確認作業
- ② 情報を開示する前に業務連携の準備を完了
- ③ 情報を開示する前にCNAを確認する
- ④ 開示しない

## ② 実務コース 【Silver】



皆さん、こんにちは。  
情報セキュリティ委員会事務局です。  
このシルバーコースはソフトバンクBBに入社された方々を対象とした基礎を学習された皆さんが対象です。  
ソフトウェアは組織的対策、物理的対策、人的対策、技術的対策と4つの基本方針の元、セキュリティ対策を講じてきました。

情報セキュリティ委員会事務局から皆さんのメッセージです。

## ④ 管理者コース 【Platinum】



修了証  
あなたは情報セキュリティ「実践コース」を修了されました。おめでとうございます。  
この修了証は、あなたの学習成果を証明するものです。大切に保管してください。

修了おめでとうです。  
「実践コース」を修了された皆さん、おめでとうございます。  
この修了証は、あなたの学習成果を証明するものです。大切に保管してください。

# 人的対策 ポータルサイトによる社内情報発信

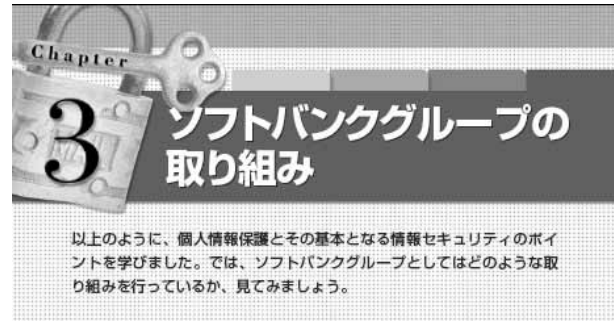


日々変化する情報をリアルタイムに全社員へ周知する為の  
情報セキュリティ委員会ポータルサイト



- 全社的イベントのマイルストーン
- 規程 / マニュアル / ガイドライン
- 各会議体議事録
- ニュース(事件の顛末)
- e - Learning
- Q & A(ナレッジベース)
- 世の中の動き
- 法律 / 制度

# 人的対策 SBグループ情報セキュリティ



## 1 ソフトバンクグループ 情報セキュリティ対策ガイドライン

ソフトバンクグループはソフトバンクBBの個人情報漏えい事件の後、こうした個人情報漏えいを二度と起こさないために、最高レベルのセキュリティを短い期間で完成しました。併せて「ソフトバンクグループ情報セキュリティ対策ガイドライン」(以下、セキュリティガイドライン)を定め、情報セキュリティ確保のための指針を設けています。

セキュリティガイドラインは次のような構成になっています。

- |                      |            |
|----------------------|------------|
| 第1章 総則               | 第8章 システム利用 |
| 第2章 情報セキュリティ体制       | 第9章 危機管理   |
| 第3章 情報資産の洗い出し及びリスク評価 | 第10章 委託管理  |
| 第4章 機密情報管理           | 第11章 契約管理  |
| 第5章 個人情報保護           | 第12章 教育    |
| 第6章 入退館管理            | 第13章 監査    |
| 第7章 システム選定           | 第14章 見直し   |

個人情報保護法の精神に基づきつつ、Chapter1、2で述べた個人情報保護と情報セキュリティ対策を規定したのが「セキュリティガイドライン」です。

## 基本方針

総則ではセキュリティガイドラインについて述べています。基本方針は以下のようになっています。

### (基本方針)

第2条 当グループ各社は事業活動を展開するうえで情報セキュリティの重要性を認識し、保有する情報資産を盗難・改ざん・破壊・漏えい・不正アクセス等の脅威から保護するため、経営者の積極的な関与のもと、情報管理体制を整備して、組織的、人的、物理的、技術的対策を講じる。特に個人情報については個人情報保護に対する社会的要請を十分に認識し、法令等を遵守するとともに個人の人權を尊重し、さらに高度な管理を実施する。以上の対策及び管理を周知徹底するため、教育及び内部監査を定期的に変更し、是正・予防処置を講じ、継続的改善に努める。

情報管理体制、とくに個人情報保護を実現するために高度な管理をすることを宣言しています。そのために、皆さんの研修/教育、監査を定期的に行うのです。

## セキュリティ体制

セキュリティ体制としては、すでにG-CISO (Group Chief Information Security Officer: グループ情報セキュリティ最高責任者)を任命し、ソフトバンクグループにおける情報セキュリティの責任者を明確にしています。

G-CISOの管轄にG-ISC (Group Information Security Committee: グループ情報セキュリティ委員会)という組織を置いています。G-ISCは、各事業統括会社の情報セキュリティ担当者によって構成される、情報セキュリティに関する諮問委員会で、情報セキュリティに関する審議、提言を行っています。

また、各事業統括会社はCISOの下に「個人情報保護管理者、監査責任者、教育担当者、苦情相談窓口担当者等を任命する」など、組織体制を整備し、役割、責任を明確化するとしています。

## 入退館管理

入退館管理は「外部との境界を適切に管理し、外来者に対してはビジターカードを発行し、外来者の記録を行う」としています。従業員が適切なIDカードを首から下げるのも、入退館管理の一環です。

ソフトバンクグループ全体(中小の子会社を含む)の情報セキュリティ対策に関するルールや決め事を、全従業員が理解するための小冊子をソフトバンク本体より配布。手元に辞書代わりに置くことにより、疑問点などを放置せずに対策を行う。



# 人的対策 ～ 個人の意識向上

### 情報セキュリティチェック強化のお知らせ

7月5日より、自主監査が毎月1回開始されます。  
各部署の担当者が、皆さんのフロアを巡回、チェックします。

#### 1. 社員証の常時携帯



- 社員証は、はっきり見える位置に携帯すること。(入退管理規程)
- カードホルダーやストラップは、正規のもの以外使用しないこと。(5月14日総務部連絡)

#### 2. 各フロア共有エリアの管理



- コピー機、ファックス機、シュレッダー周辺へ書類を放置しないこと。(情報管理規程)

#### 3. デスクの整理



- 離席時や帰宅時に、書類をデスクに放置しないこと。(情報管理規程)

#### 4. 書類の保管



- 書類（一般情報を除く）は、必ず施錠可能なキャビネット類へ保管すること。(情報管理規程)

#### 5. 貸与外パソコンの持ち込み禁止



- 貸与外パソコン（個人所有や業務委託先のパソコン）、PDAなどを社内に持ち込まないこと。(3月31日付総務部連絡)

#### 6. ノートパソコンの保管



- 離席時や帰宅時に、ノートパソコンは必ず施錠できる場所へ保管すること。(システム利用規程)

#### 7. パソコン画面の保護 (クリアスクリーン)



- パスワードで保護されたスクリーンセーバーやロック機能を設定すること。
- 離席時や帰宅時には、必ずログオフをすること。(ネットワーク管理規程)

#### 8. パスワードの管理



- パスワードやユーザーIDを付箋などでパソコンやデスク等へ貼り付けておかないこと。(ネットワーク管理規程)

## 8つの重点チェック

### 1. 社員証の常時携帯

社員証は、はっきりと見える位置に携帯すること。(入退管理規定)

### アクセス権の提示

### 2. 各フロア共有エリアの管理

コピー機、ファックス機、シュレッダー周辺  
△の書類を放置しない事。(情報管理規定)

### 3. デスクの整理

離席時や帰宅時に、書類をデスクに  
放置しないこと。(情報管理規定)

### 4. 書類の保管

書類は、必ず施錠可能なキャビネット類へ  
保管すること。(情報管理規定)

### 情報資産の管理

### 5. 貸与外パソコンの持ち込み禁止

貸与外パソコン(個人所有、委託先のPC)  
PDAなどを社内に持ち込まないこと。

### 6. ノートパソコンの保管

離席時や帰宅時に、ノートパソコンは必ず  
施錠出来る場所へ保管すること。(システム管理規定)

### 7. パソコン画面の保護 (クリアスクリーン)

パスワードで保護されたスクリーンセーバーやロック機能  
を設定すること(ネットワーク管理規定)

### 8. パスワードの管理

パスワードやユーザIDを不乾などでパソコンやデスク等  
へ貼り付けておかないこと。(ネットワーク管理規定)

### アクセス権の制御

# 社員個々人の意識

- **情報セキュリティは企業の社会的責任**
- **セキュリティリスク対策の必要性を理解する**
  - 顧客利益の保護
  - 株主・企業利益の保護
  - 企業存続性の確保
- **業務とセキュリティリスクのバランスを意識する**
  - 業務効率最優先では情報資産流出の機会を増やす
  - セキュリティ最優先では業務コストが増加する
- **情報資産の価値を正しく理解する**
  - 業務上必要な情報か
  - 情報資産価値・リスクが認識・明示されているか
  - 正しい部門・正しい人員・正しい場所で取り扱っているか
  - 保持する必要性があるか
  - 破棄する必要性はあるか

# 社員への説明

情報セキュリティ委員会 Information Web - Microsoft Internet Explorer

アドレス http://intra.sb-commerce.co.jp/division/ISC\_INFO/bio\_auth/index.html

### 登録するバイオデータについて(1)

指紋の特徴データのみを登録

原画像 → 細線化 → 特徴抽出

不可逆処理

登録/照合データ生成

3B75F48F590  
A35C7644...

画像処理後に指紋画像を削除

### 登録するバイオデータについて(2)

不可逆処理でのデータ登録

ページが表示されました



# 社員への説明

CONFIDENTIAL

新入社員用 セキュリティに伴うルール② 社外秘

使用禁止ソフトウェア 次は、使用を禁止するソフトウェアについて知りましょう。

下記は、ほんの一例でしかありません。

**Skype Winny Win-MX Softether Vir**

詳細はこちら→ ([http://intra.sb-commerce.co.jp/division/ISC\\_INFO/penalty](http://intra.sb-commerce.co.jp/division/ISC_INFO/penalty))

↓

それでは、業務上、禁止されているソフトウェアを利用しないと仕事にならない場合、どうしたらいいのでしょうか。

**申請が必要です。**  
↓ここに申請手順が書いてあります。↓  
「罰則ルール該当事項実施申請」の文字をクリックしましょう。

([http://intra.sb-commerce.co.jp/division/ISC\\_INFO/penalty/app](http://intra.sb-commerce.co.jp/division/ISC_INFO/penalty/app))

|               |      |
|---------------|------|
| ● 利用申請書 (一部抜) |      |
| 受付番号          |      |
| 進捗            | 01.4 |
| ステータス         | 作成   |
| 本部長コメント       |      |
| ISC事務局長コメント   |      |

情報セキュリティ委員会 Copyright © 2005 SOFTBANK BB CORP. All rights reserved. 9

CONFIDENTIAL

新入社員用 セキュリティに伴うルール③ 社外秘

PCや資料の社外持ち出し さあ、具体的な事例をみてみましょう！

**PCや資料の社外への持ち出しは、原則禁止です。**

外へ持ち出した時、想定される事象

例1) 登過して、電車に忘れ、ノートPCを紛失しました。  
例2) 道を歩いている、ひったくりにあい、鞆ごと持っていかれてしまいました。  
鞆の中には、携帯電話や会社の重要書類が入っていました。

その結果想定される事故

例1) ノートPCから会社の機密情報が外部へ流出しました。  
例2) 携帯電話から社員の電話番号が流出しました。  
例3) 重要書類から同業他社へ当社の動きが流出してしまいました。

↓

会社は顧客からの信頼を失い、大ダメージです。  
一度失った信頼を取り戻すのは、並大抵なことではありません！！

情報セキュリティ委員会 Copyright © 2005 SOFTBANK BB CORP. All rights reserved. 6 SoftBank BB

# ISMS認証 ~ 第三者機関による監査とPDCAの体制確認



2005年4月28日プレスリリース

## ソフトバンクBB、情報セキュリティマネジメントシステム 「BS7799-2:2002」「ISMS認証基準(Ver.2.0)」認証を同時取得 ~ 第三者機関の認定を受け、情報の安全管理をさらに強化 ~

### < 認証登録概要 >

登録組織名: ソフトバンクBB株式会社  
情報セキュリティマネジメントシステム

**規格(国際):BS7799-2:2002**

認証番号:IS93316

登録日:2005年4月15日

審査登録機関:ピーエスアイジャパン株式会社

認定機関:UKAS(英国規格協会)

**規格(国内):ISMS認証基準 Ver.2.0**

認証番号:IJ01435

登録日:2005年4月15日

審査登録機関:ピーエスアイジャパン株式会社

認定機関:JIPDEC(日本情報処理開発協会)

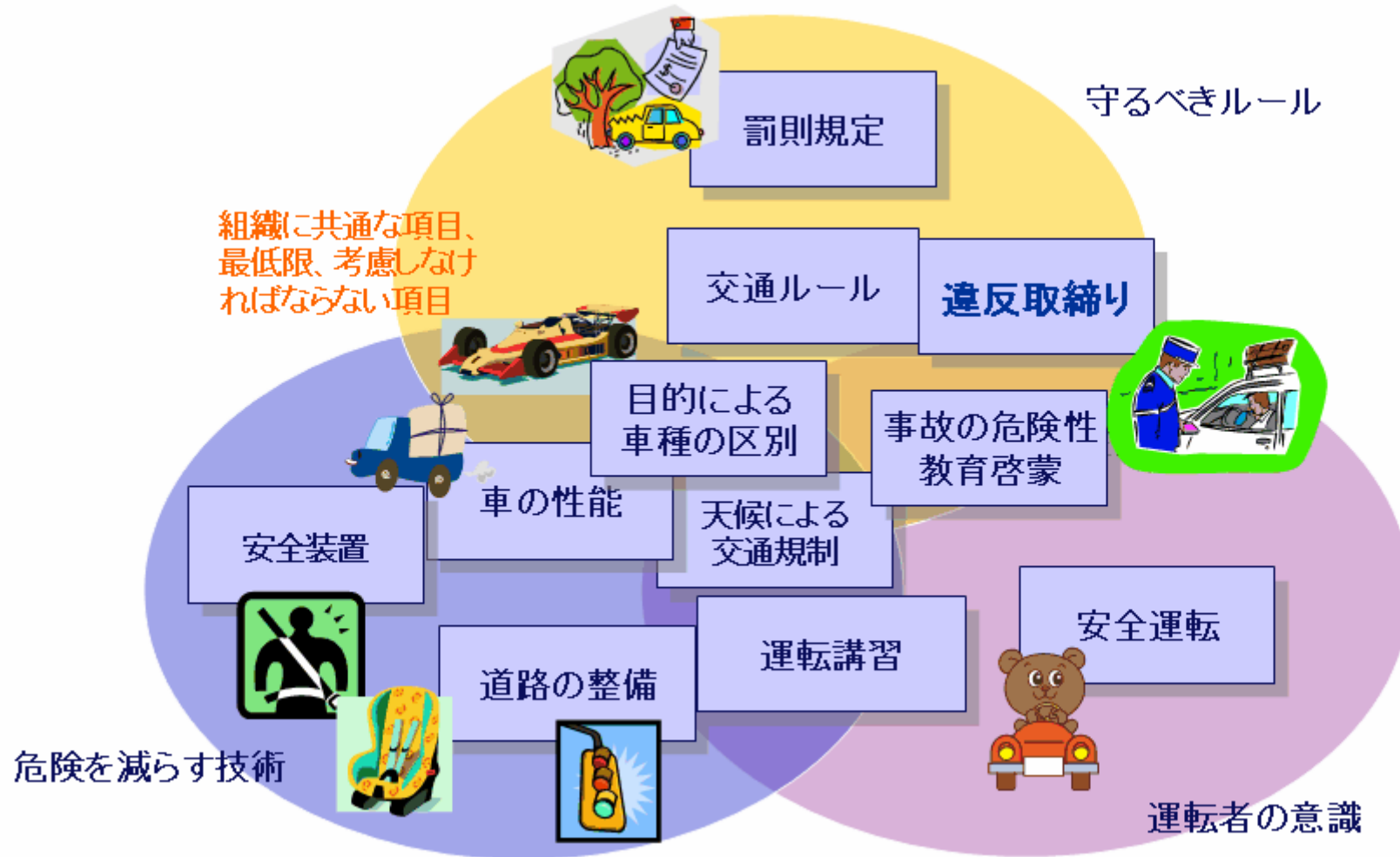
認証範囲(両規格ともに同様):

ソフトバンクBB株式会社 セキュリティオペレーションセンター(SOC)

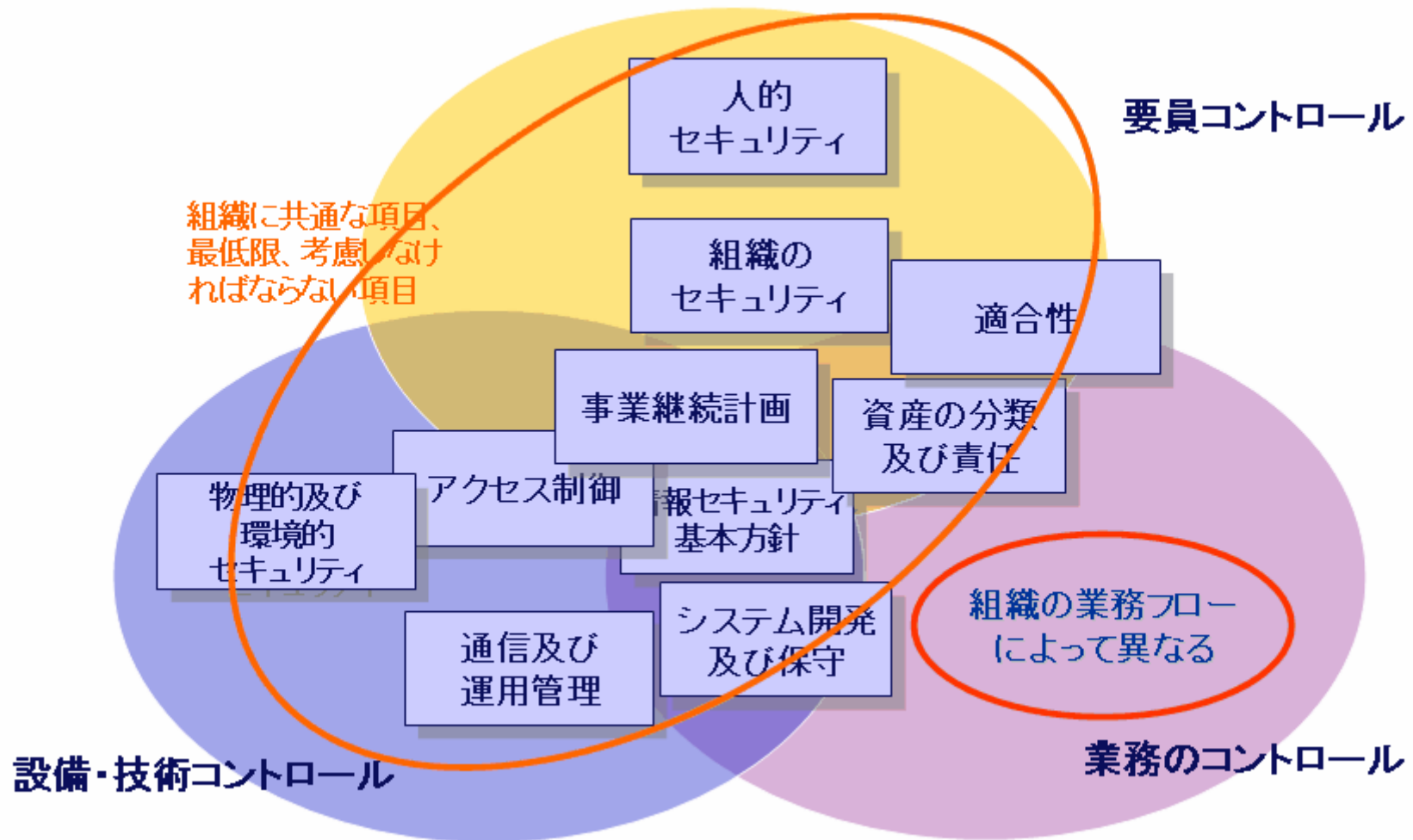
社内業務用システムの運用、システム監視及びセキュリティ監視

# 情報セキュリティ事故を防ぐには

# 交通事故を無くすには

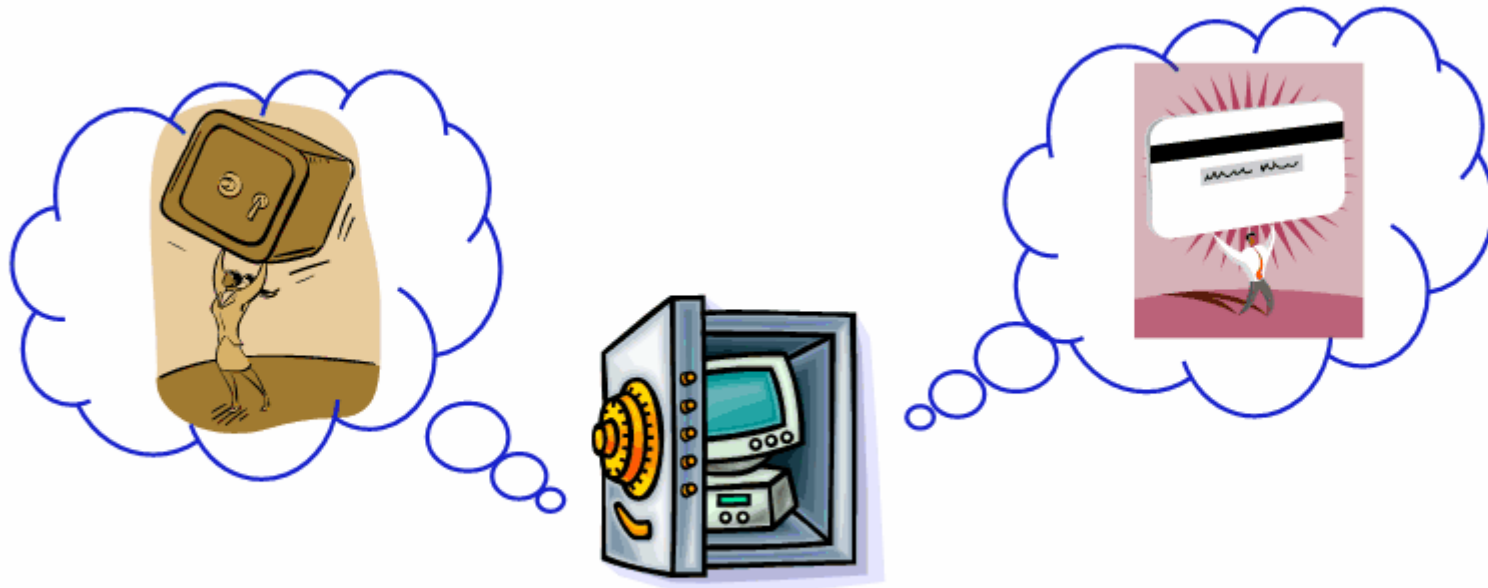


# 情報セキュリティ事故を無くすには



# 情報セキュリティの目的

情報は利用してこそ価値がある



正しい管理から信頼が生まれる

ソフトバンクBB株式会社  
<http://www.softbankbb.co.jp>

情報セキュリティに関する改善のご報告  
[http://www.softbankbb.co.jp/sbb\\_security/index.html](http://www.softbankbb.co.jp/sbb_security/index.html)