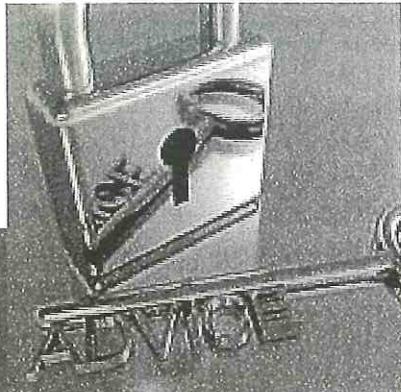


2015年度 情報セキュリティセミナー



2015年10月
情報技術開発株式会社
管理統括部
パートナー推進部

T.D.I.CO.,LTD. Technological Development of Information-processing

tcli 情報技術開発株式会社

レジメ

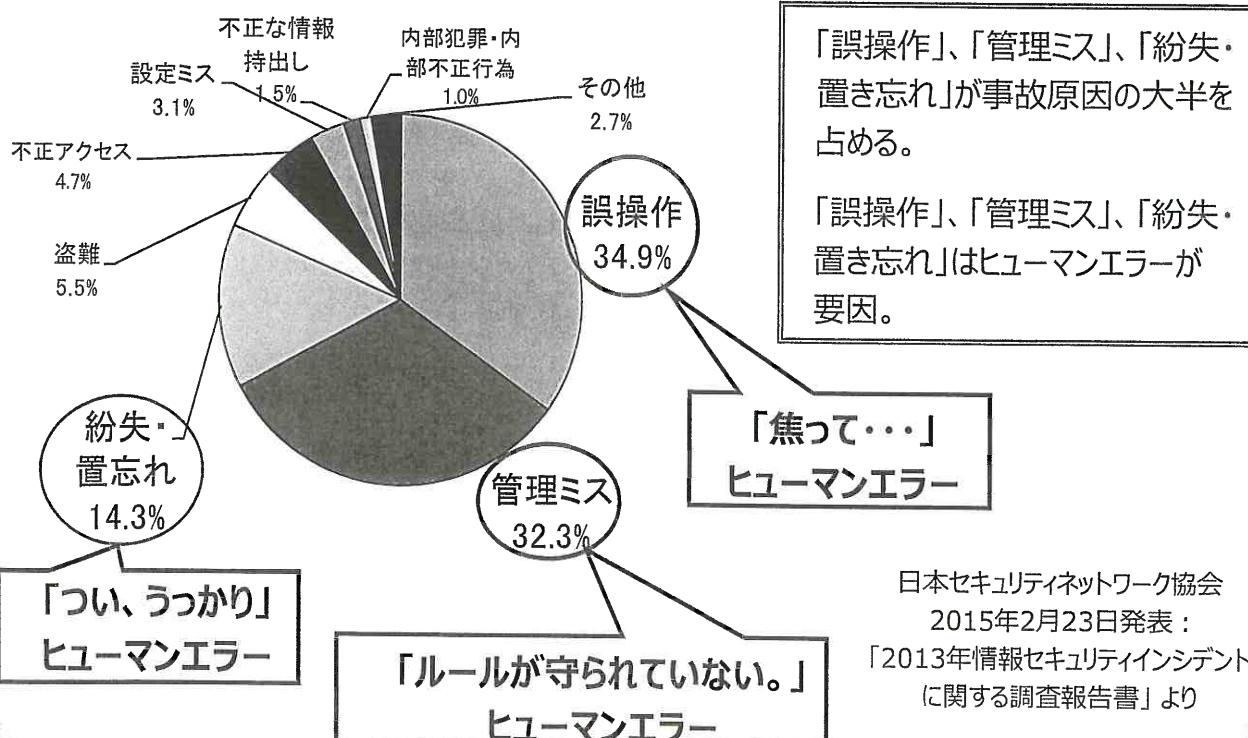
- | | |
|------------------------------------|--|
| 1. 最近の
情報セキュリティ事故 | 1 - 1 情報セキュリティ事故の原因
1 - 2 弊社グループのセキュリティ事故状況
1 - 3 ヒューマンエラーと故意 |
| 2. 事事故例からの考察 | 2 - 1 紛失
2 - 2 メール誤送信
2 - 3 ウィルス感染
2 - 4 内部不正 |
| 3. 情報セキュリティの
落とし穴・新たな脅威 | 3 - 1 落とし穴
3 - 2 新たな脅威 |
| 4. 主体的・能動的な
セキュリティ対策 | 4 - 1 情報リテラシーの育成
4 - 2 コンプライアンスの遵守 |

※対処・対策事項を記載する為
弊社グループ以外で発生した
情報セキュリティ事故例を含む

1. 最近の 情報セキュリティ事故	1 - 1 情報セキュリティ事故の原因 1 - 2 弊社グループのセキュリティ事故状況 1 - 3 ヒューマンエラーと故意
2. 事故事例からの考察	2 - 1 紛失 2 - 2 メール誤送信 2 - 3 ウイルス感染 2 - 4 内部不正
※対処・対策事項を記載する為 弊社グループ以外で発生した 情報セキュリティ事故事例を含む	
3. 情報セキュリティの 落とし穴・新たな脅威	3 - 1 落とし穴 3 - 2 新たな脅威
4. 主体的・能動的な セキュリティ対策	4 - 1 情報リテラシーの育成 4 - 2 コンプライアンスの遵守

1. 最近の情報セキュリティ事故

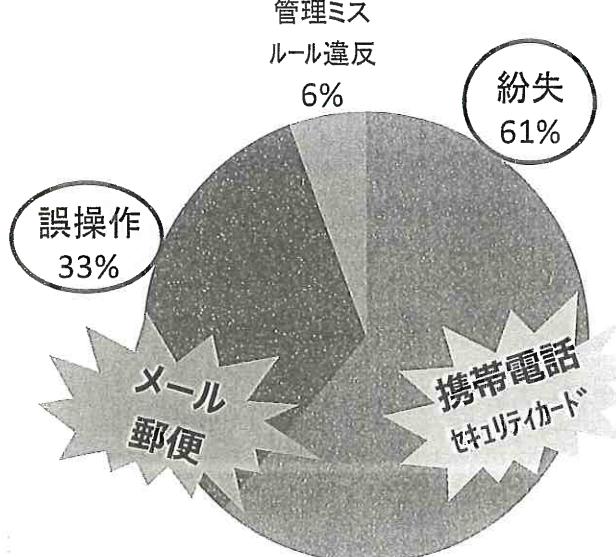
1 - 1 2013年 個人情報漏えい事故の原因



1. 最近の情報セキュリティ事故

1-2 弊社グループのセキュリティ事故状況

■弊社グループのセキュリティ事故原因



■弊社グループの事故原因の傾向と特徴

- 区分では「紛失」、「誤操作」が多い。(継続)
- 原因では、「紛失」は不注意や所持確認を怠る、「誤操作」は確認を怠る事等。

《ほとんどの事故が過信と油断による
ヒューマンエラー
によって発生している!》

従業者一人一人が自主的に、
改善や対策を実施しなくては、
事故を防ぐことはできない。

1. 最近の情報セキュリティ事故

1-3 ヒューマンエラーと故意

うっかり



- 酔いつぶれて、パソコンやモバイル端末の入った鞄を紛失
- お客様貸与スマートフォンや携帯電話の紛失
- メールの添付資料間違い
- メールの宛先間違い
- SNSに顧客情報を掲載

知らないうちに

- Webシステム開発サーバーに不正アクセス
- パートナー社内情報が一般公開状態



故意



- お客様のキャッシュカードを偽造
- お客様の会員情報を詐取

1. 最近の 情報セキュリティ事故	1 - 1 情報セキュリティ事故の原因 1 - 2 弊社グループのセキュリティ事故状況 1 - 3 ヒューマンエラーと故意
2. 事故事例からの考察 ※対処・対策事項を記載する為 弊社グループ以外で発生した 情報セキュリティ事故事例を含む	2 - 1 紛失 2 - 2 メール誤送信 2 - 3 ウイルス感染 2 - 4 内部不正
3. 情報セキュリティの 落とし穴・新たな脅威	3 - 1 落とし穴 3 - 2 新たな脅威
4. 主体的・能動的な セキュリティ対策	4 - 1 情報リテラシーの育成 4 - 2 コンプライアンスの遵守

2. 事故事例からの考察

再び事故を起こさないために……

■原因と要因と理由

原因とは、今回の事象を発生させたもの

要因とは、ある事象に大いに影響があるもの

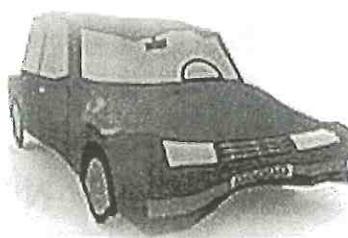
理由とは、物事がそのようになってしまったわけ

例) 事象：交通事故を起こしてしまった

原因：居眠り運転

要因：睡眠不足 (理由：前日遅くまで深酒をした)

理由：疲労 (理由：連日、深夜残業が続いた)



■問題と課題

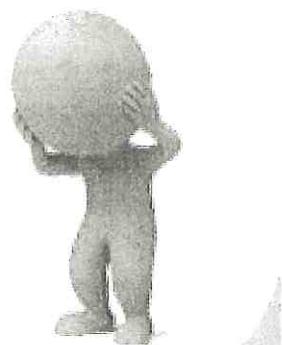
問題とは、現状(実際の姿)と、目標(あるべき姿)との
差異(具体的な事象)

課題とは、問題を解決するために、行動を起こすことを
意思表明したもの

例) 事象：交通事故を起こしてしまった

問題：疲れると眠くなる

課題：疲れない、又は疲れても事故を起こさない環境作り



2. 事故事例からの考察

事故事例（1）～酔いつぶれてパソコン・入館証の入った鞄を紛失～

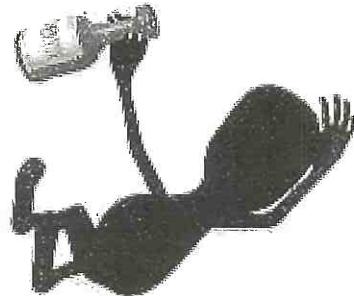
■ 概要

- お客様訪問後、数件で飲食し泥酔。自宅にどう帰ったかも不明。
- 翌日、目が覚めて鞄が無いので仰天！



■ 経緯・状況

- 上司に報告後、所轄の警察に紛失届を提出。
- 翌日、飲酒した店より鞄を忘れているとの連絡が入る。
- PCは、HDDパスワードとWindowsパスワードを設定。
- PCにお客様の取り引きデータ、案件情報を保管。



■ 対処・対策

- 入館証の無効化を依頼。
- 紛失して戻ってきたパソコンのアクセス履歴を調査。
- パソコンのセキュリティ対策、持出しルールの見直し。
- パソコン保管されたデータの廃棄・削除。
- セキュリティ規則の再周知徹底。

2. 事故事例からの考察

事故事例（2）～顧客貸与スマートフォンの紛失～

■ 概要

- システムサポートの連絡用として、お客様からスマートフォンを貸与されていた。
- 滅多に使用していなかったため、紛失に気付かなかった。

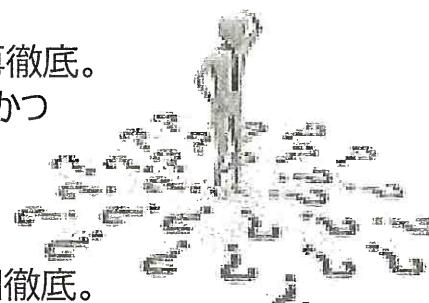


■ 経緯・状況

- リサイクルショップからのパスワード解除依頼を不審に思ったキャリアからお客様に連絡が入り、紛失していることが発覚。

■ 対処・対策

- 不用意な持出しと貸与品に対する管理意識の再徹底。
- お客様ルールにより、パスワードロックが設定され、かつ電話番号/メール/文書などが保存していなかったため、情報漏洩のリスクは少ないと判断された。
- お客様へ謝罪。
- 持出しルールの見直し。セキュリティ規則の再周知徹底。
- 首かけストラップの装着をルール化。



2. 事故事例からの考察

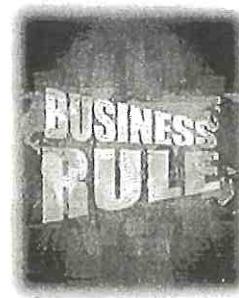
事故事例から要因を考えてみましょう！



■ 機密情報の持ち出しているという意識が低い。

- 案件情報を出した際の紛失・盗難対策が取られていない。
- 検収が完了した案件情報も削除せずに保持している。

■ ルールを遵守しなくても指摘されない職場環境。



■ 紛失・盗難に遭遇していない自分は、大丈夫だという過信。

■ お客様に信頼があるSEが事故を起こしている。
→ 幅広い業務をこなす分、リスクが多くなる。

2. 事故事例からの考察

紛失・盗難にあわない



- 体、目から離さない。
- 電車乗車時は、網棚、足元に置かない。
- 持出し時に、許可を得る。
- 携帯して、飲酒をしない。
- 鞄のたすき掛け、ストラップをベルトに通す等。
- 防犯ブザーを装着する。



紛失・盗難にあった場合の被害を最小化する

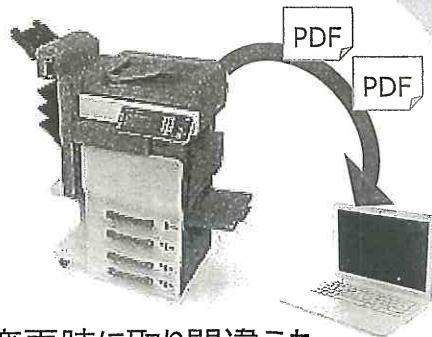
- 持出す情報は、必要最小限にする。
- 持出し専用のセキュリティ対策を講じた機器を使用する。
- ディスク全体を暗号化、スマートデバイスは、パスワードを設定する。
- 持出し情報は申請書・台帳に記入しておく。
- 所轄の警察等に直ちに届ける。
- エスカレーションルールに基づき、直ちに報告する。
- ローカル/リモートワイプ、ローカル/リモートロックを設定する。

2. 事故事例からの考察

事故事例（3）～メール添付資料の誤り～

■ 概要

- ・パートナー担当者が、A社とB社各々にメールで資料を送る際に、添付資料を双方逆に送付した。（A社からの連絡で発覚）



■ 経緯・状況

- ・送付文書を複合機でPDF化、その後ファイル名の変更時に取り間違えた。
- ・A社、B社に添付資料の内容を再確認せずにメールに添付し送信した。

■ 対処・対策

- ・A社、B社へ謝罪と削除を依頼し、削除確認を実施。
- ・添付ファイルの送信時、宛先/添付ファイルの再確認等社内教育を再実施。
- ・設定時に声を出して確認する。
- ・月次で実施しているセキュリティチェックのチェック項目に追加。



2. 事故事例からの考察

事故事例（4）～メール宛先間違い～

■ 概要

- ・お客様先でシステムエラー連絡を担当の社員へメールで自動送信されるようにしたが、担当社員のアドレスを誤って、同姓同名の別部門の社員を設定してしまった。
- ・後日お客様の本社から当該事業所に連絡が入り発覚。



■ 経緯・状況

- ・オートコンプリート機能を使用したが、よく確認しないで選択した。
- ・大企業のために、宛先の誤設定が発覚するまでに時間がかかった。

■ 対処・対策

- ・お客様（当該部署と間違えた部署）への謝罪。
- ・宛先の再設定。
- ・設定時再確認の周知徹底。
- ・設定時に宛先のアドレスを声に出して確認する。
- ・月次で実施しているセキュリティチェックのチェック項目に追加。



2. 事故事例からの考察

事故事例（5）～個人SNSに顧客情報を掲載～

■ 概要

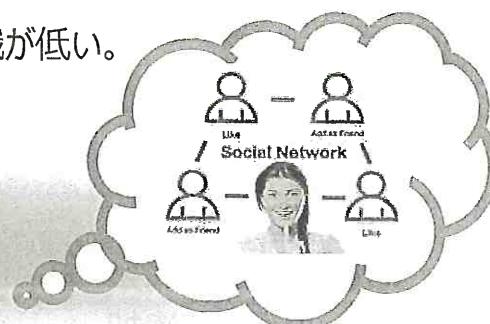
- ・Aパートナー企業のB氏が、個人のSNSにエンドユーザー名や業務名等を掲載。
- ・お客様担当者がB氏のSNSを閲覧して、委託業務名等情報漏洩を発見。

■ 経緯・状況

- ・B氏のSNSは、全てに公開の設定で使用。
- ・SNS記事へのアクセスログ無しの設定のため、
アクセス者は特定できず。
- ・受託業務における「機密情報」の取扱い意識が低い。

■ 対処・対策

- ・掲載記事削除、SNSアカウント削除。
検索エンジン、まとめサイト等の監視。
- ・お客様へ謝罪及び対処等報告。
- ・個人利用のSNSガイドラインの周知徹底。
- ・社内教育の実施。



2. 事故事例からの考察

事故事例から要因を考えてみましょう！



■ 機密情報を社外に持ち出せる (発信できる) という意識が低い

- 多忙、煩雑だから、注意力が散漫に
- メール送信手順（宛先確認、添付ファイル確認等）
を守っていない
- 慣れによる過信（緊張感の低下）



■ メール送信手順が個人に依存

■ 送信ツール導入、運用ルール策定では限界有り



2. 事故事例からの考察

誤送信しない

●宛先、添付ファイル

- ・アドレス帳の目的別(顧客別等)に分ける。
- ・設定した宛先は、声を出して確認する。
- ・極力、「返信」で送るようにし、宛先に間違いがないか再確認(返信不要な宛先は削除)。
- ・送信時に一時保留の設定にし、送信処理前に宛先、平文、添付ファイルの中身を再確認する。
- ・受信した電子メールの自動アドレス登録機能を禁止する。



誤送信した場合の被害を最小化する

●共通

- ・不要な平文(何回も受送信した履歴文等)は、削除する。

●宛先

- ・同報先は、CCではなく、BCCにする。
- ・不要な宛先は削除する。
- ・全員に返信する場合は、宛先全員が妥当か確認する。

●添付ファイル

- ・暗号/パスワードを必ず付加する。
- ・極力、相手のみ推察可能なキーをパスワードで用い、パスワード通知メールに明記しない。
- ・添付ファイルを送付した同一メールに、パスワードを明記しない。



2. 事故事例からの考察

事故事例（6）～Webシステム開発サーバーに不正アクセス～

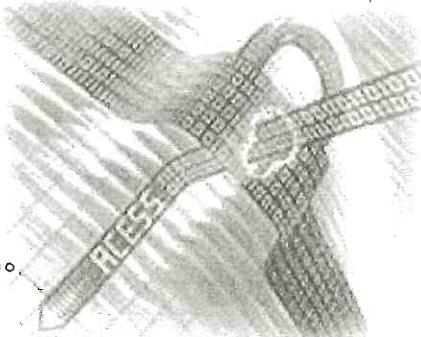
■概要

- ・パートナー社内に設置したテスト用Webシステム二、第三者が不正アクセス。
- ・開発機のroot、Oracleパスワードが変更、ログ/データ等が削除、不明アプリの実行。



■経緯・状況

- ・接続テストの為、ファイアウォールのセキュリティポリシーを変更し、不要なプロトコルも遮断しなかった。
- ・開発機にrootログインができなくなり発覚。



■対処・対策

- ・ファイアウォールログ解析、お客様へ謝罪。
- ・セキュリティ関連作業実施手順書の整備と徹底。
- ・実施体制、処理手順の詳細定義、事前報告 他。
- ・開発機器環境のセキュリティ強化。
- ・rootログイン制御、ログ監視 他。

2. 事故事例からの考察

事故事例（7）～A社の社内情報が一般公開状態～

■概要

- ・社外から閲覧可能な自社のコミュニケーションシステムが一般公開されていた。
- ・アクセスログより検索エンジン他により閲覧された形跡あり。

■経緯・状況

- ・終了したプロジェクトの情報を保持。
- ・A社のドメイン名で、httpアクセスして発覚。

■対処・対策

- ・外部からのアクセスを遮断。
- ・Google、Yahoo、goo、bingの検索キヤッショの削除。
- ・Web環境の変更、システム確認ツールの強化。
- ・是正後に外部セキュリティ診断を受診
⇒ 事故是正監査を実施。

ウイルス感染



2. 事故事例からの考察

事故事例から要因を考えてみましょう！



- 納期や生産性を優先するあまり、
お客様、自社の大切なデータを
取り扱っているという意識が低くなってしまう。
 - －人材育成が十分に行われていない
 - －社内に支援・チェックする体制、ルールがない

■個人のスキルに依存

- －スキルがなくても使えてしまうシステム
(ブラックボックス化)
- －不正アクセスの実情を把握していない

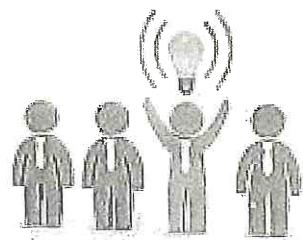


2. 事故事例からの考察

感染させない

●共通

- ・O S、ソフトウェア、ウイルスパターンファイルは、常に最新化。
- ・最低1回／月もしくは週は、全スキャンを実行。



●メール

- ・テキスト形式のみで送受信（HTMLメールは送受信しないように設定する）。
- ・不審なメール（知らない送信元、おかしい日本語等）は、添付ファイルを開かない。
- ・迷惑メールフィルターのレベルを設定する。

●Web

- ・仕事に無関係なサイトは見ない。
- ・フリーソフトはインストールしない。

感染した場合の被害を最小化する

●共通

- ・パソコンが不審な動きをした場合、直ちにネットから遮断し、情報セキュリティ事務局等に連絡する。
- ・現状を保持し、自分で対処しない。専門部門に指示を仰ぐ。



2. 事故事例からの考察

事故事例（8）～顧客のキャッシュカードを偽造～

■概要

- ・システムログから、ID、パスワードをもとに偽造カードを作成。
- ・A T Mより金銭を詐取。

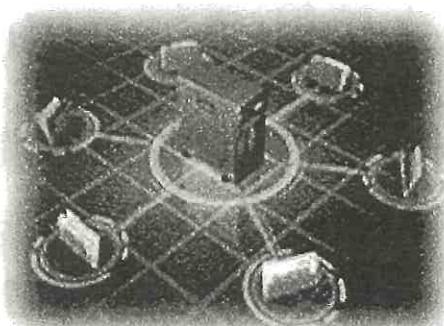


■経緯・状況

- ・システムログ、危機管理の甘さ。
- ・権限が集中していた。異動が無く長年同じお客様をサポートし、内部事情に精通。
- ・分相応以上の生活のため困窮。

■対処・対策

- ・体制変更、規程改定。
- ・教育の徹底。
- ・刑事告訴。

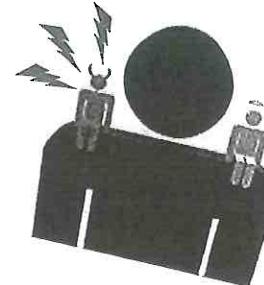


2. 事故事例からの考察

事故事例（8）～顧客の会員情報を詐取～

■ 概要

- ・技術に詳しく重宝され、大半の権限を与えられていたS.E.が、派遣先の社内データベース内の顧客情報を外部に持ち出し、名簿業者に売却した。
- ・別会社からのダイレクトメールが届くようになり発覚した。



■ 経緯・状況

- ・会社の貸与ノートパソコンから充電しようとスマートフォンのケーブルを差したら、セキュリティー上の欠陥から反応したことから、金銭目当てに顧客情報を持出した。不正競争防止法違反で逮捕。



■ 対処・対策

- ・個人情報漏洩被害者へ補償（約260億円）。
- ・第三者による調査委員会の設置。
- ・グループ内の組織体制の再構築。
- ・コンプライアンス教育の徹底。
- ・集団訴訟対応。

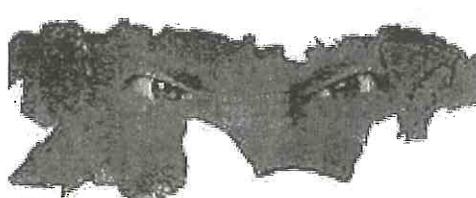
2. 事故事例からの考察

事故事例から要因を考えてみましょう！



■ 個人的問題

- －不満（環境、報酬、人間関係、金銭、同じ仕事）
- －自己中心的、バレないという過信
- －借金、ギャンブル、交友



■ 環境、組織

- －仕事が個人に依存し、配置転換が難しい
- －権限が集中している
- －性善説に基づく対策のみ

■ 権限がある人の悪意を防ぐのは難しい

- －正規のアクセス権限を持っていれば、技術的対策は難しい

2. 事故事例からの考察 【参考情報】

内部不正が発生する要因

順位	内 容	割合
1	不当だと思う解雇通告を受けた	34.2%
2	給与や賞与に不満がある	23.2%
3	社内の人事評価に不満がある	22.7%
4	職場で頻繁にルール違反が繰り返されている	20.8%
5	システム管理がズさんで顧客情報を簡単に持ち出せる事を知っている	20.1%
6	社内ルールや規則に違反した際、罰則がない	18.7%
7	上司の仕事の取組み方や上司の人間性に不満がある	18.3%
8	職場で人間関係のトラブルがある	17.8%
9	社内の誰にも知られずに、顧客情報などの重要な情報を持ち出せる方法を知っている	16.4%
10	かつて同僚がルール違反を行ったことが発覚したが、社内で処罰されなかつた	16.1%

出展：IPA 組織内部者の不正行為によるインシデント調査 調査報告書2012年7月

資料：<http://www.ipa.go.jp/files/000014169.pdf>

2. 事故事例からの考察 【参考情報】

内部不正を起こす要因

人が不正行為を実行するに至る仕組み
(米国犯罪学者D.R.クレッシー著)

不正のトライアングル

不正行為は、(1)機会、(2)動機、(3)正当化
という3つの不正リスクが揃った時に発生する。

要因の理解

(1)機会

不正を犯す機会、職場環境があることを指す。

ex.請求業務と入金業務を同一人物が担当という環境。

やろうと思えば
できる環境

不正行為しか
見えなくなった心情

(2)動機

不正行為を実行するしかないと考えるに至った事情を指す。

ex.横領する動機「借金返済に追われている」などの事情。

「誰にも相談できない」に端を発するケースも多い。

(3)正当化

自ら納得させる理由付けを指す。

ex.「短時間だから」「仕方がない」など自分に
都合の良い理由をこじつけること。

「良心の呵責」
を乗り越える

2. 事故事例からの考察

内部不正させない

- 不正アクセスを隠蔽しても、発覚する環境であることを周知する。

- ・物理的監視 (ex.情報保管、入室管理、監視カメラ、機器接続等)

- ・技術的監視 (ex.アクセス制御、稼動・操作ログ等)

- ・不適切な書き込み (ex.SNS、ブログ等)

具体例 (フォレンジクス/forensics)

- ・ハードディスク、USBメモリ内データの一般的な削除方法では、復旧可能

- ・イベントログに、ログイン情報、USB接続機器等が自動記録

- ・F/W等のネットワークログに、通信履歴が記録



- 社内規定・契約の整備、モラルの育成

- ・委託元と自社間の契約事項と同等の契約内容で、

- 再委託先と契約を実施。

- ・退職者対策を確実に実施。

- ・情報セキュリティモラルの周知徹底。



機会、動機を排除する対策

フォレンジクス：不正アクセスや機密情報漏洩等コンピュータ関連の犯罪や法的紛争の発生時に、原因究明や捜査に必要な機器やデータ、電子的記録を収集・分析し、その法的な証拠性を明らかにする手段や技術。

レジメ

1. 最近の 情報セキュリティ事故

- 1 - 1 情報セキュリティ事故の原因
- 1 - 2 弊社グループのセキュリティ事故状況
- 1 - 3 ヒューマンエラーと故意

2. 事故事例からの考察

※対処・対策事項を記載する為
弊社グループ以外で発生した
情報セキュリティ事故事例を含む

- 2 - 1 紛失

- 2 - 2 メール誤送信

- 2 - 3 ウイルス感染

- 2 - 4 内部不正

3. 情報セキュリティの 落とし穴・新たな脅威

- 3 - 1 落とし穴
- 3 - 2 新たな脅威

4. 主体的・能動的な セキュリティ対策

- 4 - 1 情報リテラシーの育成
- 4 - 2 コンプライアンスの遵守

3. 情報セキュリティの落とし穴・新たな脅威

落とし穴①

■ PC・スマートデバイスのリモートワイフ[®]

- ・紛失、盗難の発覚から、リモートワイフ処理までにタイムラグがある。
- ・電波が届かないところや、通信機能をオフにされると処理できない。
- ・リモートワイフが完了したかは、現物でしか確認できない。
- ・外部ディスク、SDカードは対象外。

対策 →

- ・PC、スマートデバイス内の情報を明確にする。
- ・使われ方、使い方を明確にする。
- ・MDMソフトの機能を確認する。



3. 情報セキュリティの落とし穴・新たな脅威

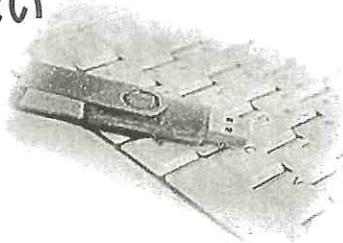
落とし穴①

■データは削除したつもりでも実は消えていない

- ・復元・修復ツールでほぼ再読み込み可能。

対策 →

- ・データ上書きツールを使用。
- USBメモリは削除できない場合あり。
- ・物理的に完全破壊。

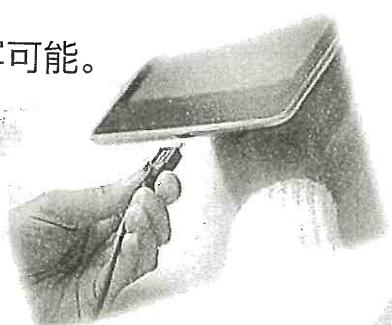


■パソコンからのスマホの充電。実はデータコピー？

- ・データ転送可能なUSBケーブルを接続していれば複写可能。

対策 →

- ・USBポートを無効化。
-接続プロトコルによっては接続禁止
設定が効かない場合あり。
- ・USB接続イベントログを収集。



3. 情報セキュリティの落とし穴・新たな脅威

落とし穴②

■スマートデバイスの不正アプリ

- ・「このアプリケーションに許可する権限」を確認。
-ネットワークアクセス、ストレージ、電話/通話、
電話帳、GPS、アカウント…

対策 →

- ・評判だけでなく、レビュー、作成元も確認。
→ それでも巧妙な不正アプリはある。



■ウイルス対策ソフトだけで、完全に防御しきれない

- ・1日平均で約100万種類の新種、亜種が登場。
- ・ウイルスの短命化、感染先を限定。
- ・パターンファイルの配布が間に合わない、完璧でない。

対策 →

- ・OSの最新化、怪しいサイト/メールは見ない等複数の対策をとる。
→ それでもウイルスに感染する可能性はある。



3. 情報セキュリティの落とし穴・新たな脅威

落とし穴②

フリースポット

■無線公衆 LAN

- ・暗号化されていない通信は、盗聴できるのは当たり前。
- ・公衆無線 LAN で安全が保証されないのは当然で、
サービスに落ち度はない。
- ・暗号化したところでサービス提供のために鍵を共有
すればパケットキャプチャができる。



対策 →

- ・情報漏洩リスクを考慮し、クレジット
カード番号など大事なやりとりはしない。
→ 知らないうちに盗聴されて
いる可能性がある。



3. 情報セキュリティの落とし穴・新たな脅威

新たな脅威

- ウェアラブル端末
- IoT (Internet of Things)、M2M (Machine-to-Machine)
- マイナンバー
- ビッグデータを活用するために法改正（2015年個人特定性低減データ）
- オープンデータ（公共）による、個人の特定

2013～	スマート家電	
2013/11	Amazonがドローン配送サービス構想を発表	
2014/ 3	IoTの標準化団体	
2014/ 4	Googleが自動走行車のプロトタイプを公開	
2014/ 4	Google Glass米国で発売開始	
2015/10	行政手続における特定の個人を識別するための番号の利用等に関する法律	
2016/ ?	個人情報保護法の改正 (マイナーバー)	

レジメ

- | | |
|----------------------|---|
| 1. 最近の
情報セキュリティ事故 | 1-1 情報セキュリティ事故の原因
1-2 弊社グループのセキュリティ事故状況
1-3 ヒューマンエラーと故意 |
|----------------------|---|

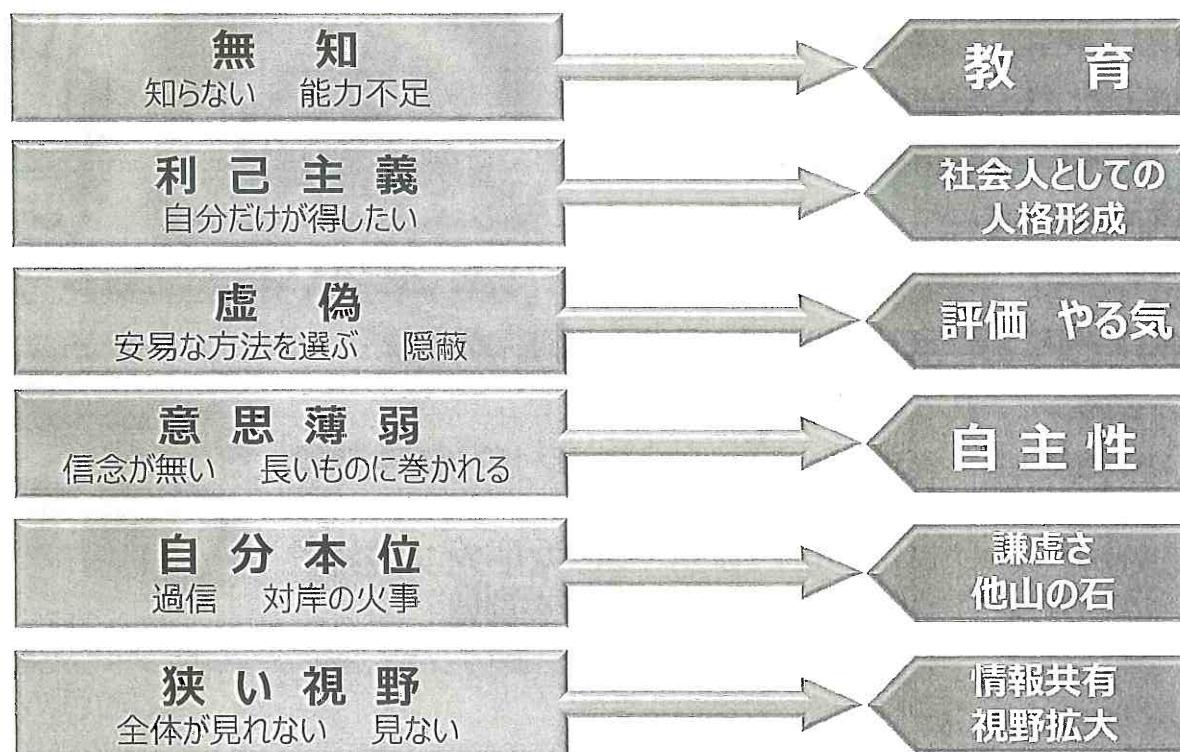
- | | |
|--------------|--|
| 2. 事事故例からの考察 | 2-1 紛失
2-2 メール誤送信
2-3 ウィルス感染
2-4 内部不正 |
|--------------|--|
- ※対処・対策事項を記載する為
弊社グループ以外で発生した
情報セキュリティ事事故例を含む

- | | |
|----------------------------|-----------------------|
| 3. 情報セキュリティの
落とし穴・新たな脅威 | 3-1 落とし穴
3-2 新たな脅威 |
|----------------------------|-----------------------|

- | | |
|-------------------------|-----------------------------------|
| 4. 主体的・能動的な
セキュリティ対策 | 4-1 情報リテラシーの育成
4-2 コンプライアンスの遵守 |
|-------------------------|-----------------------------------|

4. 主体的・能動的な対策

4-1 情報リテラシー（プロ）の育成

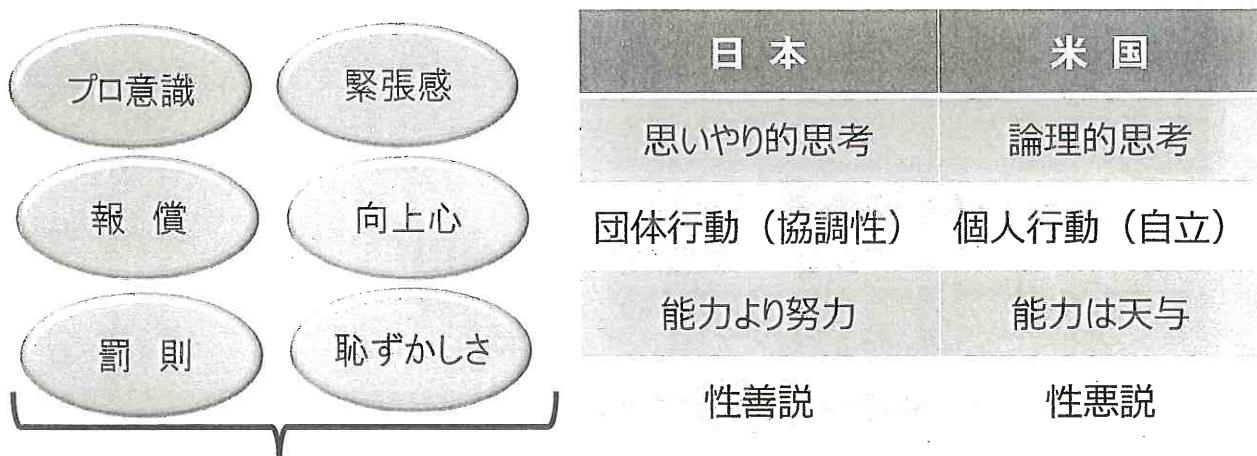


35

tdi 情報技術開発株式会社

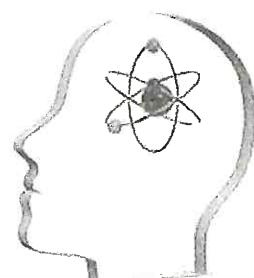
4. 主体的・能動的な対策

4-1 情報リテラシー（プロ）の育成



あなたの、その考え方、行動

- お客様、上司、家族に自慢できますか？
- 見つからなければ大丈夫だと思っていませんか？
- 第三者から見て、どう思いますか？



4. 主体的・能動的な対策

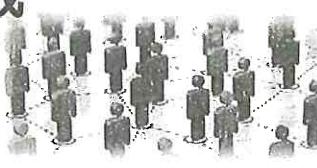
4-1 情報リテラシー（プロ）の育成

■個人特性とインシデント

■情報セキュリティ知識とインシデント発生確率

- ・パソコン、USBメモリ紛失 知識のある人の方が個々の確率が高い。
⇒ 外出頻度、保有率、使用頻度が高い。
- ・メール誤送信 知識には関係が無い。

→ 教育・研修と誓約書により、インシデントは減少する。



■行動特性とインシデントの関係

- ・遅刻や勘違いが多かったり、業務に関係ない書き込み、雑談等をする人の方が確率が高い。
- ・業務多忙だとインシデントが発生しやすい。



→ ルール違反が常態化すると、インシデントが発生しやすくなる。

ICTのプロは、情報セキュリティリスクが高い！

4. 主体的・能動的な対策

4-1 情報リテラシー（プロ）の育成



企業内での社員教育研修などで利用できるように、情報セキュリティ読本 四訂版に準拠した教育用スライド資料

<https://www.ipa.go.jp/security/publications/dokuhon/ppt.html>

情報セキュリティに関する脅威や対策などを学んで頂くための映像コンテンツを、YouTube内の「IPA Channel」を通じて公開しています。

<https://www.youtube.com/user/ipajp>



IPA_5分でできる
情報セキュリティ
ポイント学習

http://www.ipa.go.jp/security/keihatsu/pr2012/tech/040_5minlearning.html

主に中小企業で働く方を対象とした、情報セキュリティについて、勉強できる無料の学習ツール。

4. 主体的・能動的な対策

4-1 情報リテラシー（プロ）の育成



トレンドマイクロが運営するセキュリティ情報サイト。

スマートフォン、クラウド、フィッシング詐欺、ワンクリック詐欺、迷惑メールなどのセキュリティ対策、最新のセキュリティニュースを提供。

<http://www.is702.jp/>



日立製作所が配信している中小企業のセキュリティ管理のためのリスクを未然に防ぐ「セキュリティ管理」と「IT資産管理」の重要性について、マンガで分かりやすく解説。

<http://www.hitachi.co.jp/Prod/comp/soft1/itoperations/feat/comic/>

39

tdi 情報技術開発株式会社

4. 主体的・能動的な対策

4-1 情報リテラシー（プロ）の育成



JPCERTコーディネーションセンター（JPCERT/CC）は、企業や組織の教育担当者や情報セキュリティ担当者を対象に、新人教育用の情報セキュリティ資料を無償で公開。

<http://www.jpcert.or.jp/magazine/security/newcomer.html>

tdi 作成研修資料
(2015年度版)



3. 情報セキュリティ事故事例

事故事例（8）～顧客のキャッシュカードを偽造～

- 概要
 - システムログから、ID、パスワードとともに偽造カードを作成、ATMより現金を詐取。

経緯・状況

- システムログ、在籍管理の日記。
 - 顧客が銀行で、当館が銀行と同様にカードを保持し、内部規則に従う。
 - 分明以上的生活のため顧客。

対処・対策

- 体制変更、内規改定
- 教育実施
- 対応報告

6. 事故対応

紛失や盗難などの緊急事態が生じた場合は、

直ちに

所属の上司、セキュリティ担当に連絡する。

※必ず緊急連絡体制を確認しておく



関係者へ連絡する。

お客様、パートナー様、警察（交番）、利用交通機関等

※事故については明確に連絡をしましょう。

SW1H -だい(who) -いつ(when) -どこで(where)

-どうして(How) -どのような(what)

4. 主体的・能動的な対策

4-2 コンプライアンスの遵守

- 不正競争防止法
- 刑法
- 不正アクセス行為の禁止等に関する法律
- 著作権法
- マイナンバー法施行
- 個人情報保護法改正
- 労働者派遣法改正
- 関係省庁のガイドライン



いつでも見れる工夫を！



本日は、ご清聴ありがとうございました。

弊社グループはお客様の満足を第一に考え、
高品質の製品・サービスを将来にわたり
提供することで社会に貢献いたします。

引き続きご支援、ご協力賜りますよう
よろしくお願ひ申し上げます。

