情報セキュリティーと人権

中小企業担当者向け
90分

WEB110.COM
吉川誠司

「CODE BLUE 2015」の全講演タイトルの一例

- シンギュラリティがやってくる
- 実用的な大規模ネットワークのディフェンスあるいは「Eierlegende Wollmichsau」の保護
- マハラジャの最後通告、「バザール」と未来への影：ゼロデイマーケットにおける強要と協力
- 現実世界での機械学習によるアノマリ検知システムの構築と回避
- APTで使用されたバイナリの相関解析忍術
- あなたのAppleにもEFIモンスターはいませんか？
- X-XSS-Nightmare: 1; mode=attack ～XSSフィルタを利用したXSS攻撃～
- PANDEMONIUM: 動的バイナリ計測とファジーハッシュを使用した暗号アルゴリズムの自動識別
- mmapを用いたスタックカナリア回避手法の提案

https://www.jitec.ipa.go.jp/sg/

次のような方に受験をお勧めします！

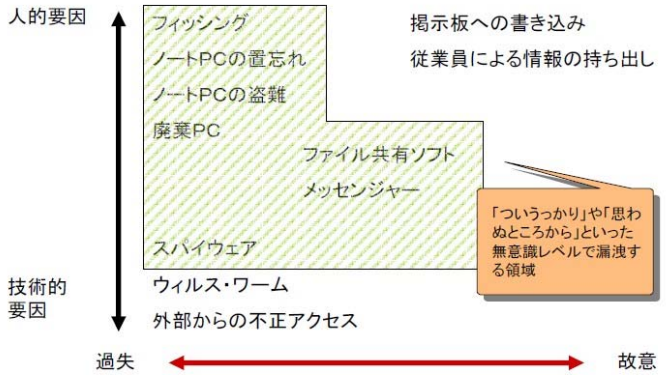
Target 01	業務で個人情報を取り扱う全ての方
Target 02	業務部門・管理部門で情報管理を担当する全ての方
Target 03	外部委託先に対する情報セキュリティ評価・確認を行う全ての方
Target 04	情報セキュリティ管理の知識・スキルを身に付けたい全ての方
Target 05	iパス（ITパスポート試験）合格から、さらにステップアップしたい全ての方

組織と個人の情報を守るための

5つのポイント

1. 情報漏えいの原因と経路を知る
2. 情報奪取の攻撃方法を知る
3. スマホ・タブレットからの漏えいリスク
4. SNSのプライベート利用を甘く見ない
5. 情報漏えい対策６か条

企業で発生する情報漏えいの分類



2013年　個人情報漏えいインシデントTOP10

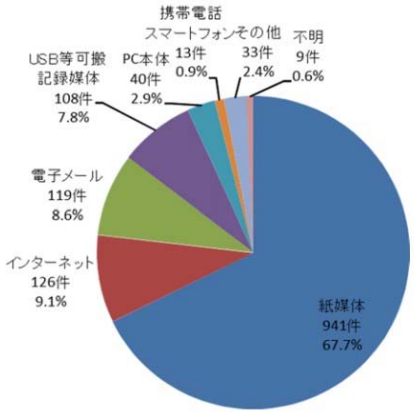
No.	漏えい人数	業種	原因
1	400 万人	情報通信業	不正アクセス
2	169 万 2496 人	情報通信業	不正アクセス
3	47 万人	卸売業，小売業	不正アクセス
4	42 万 6000 人	公務(他に分類されるものを除く)	紛失・置忘れ
5	24 万 3266 人	情報通信業	不正アクセス
6	17 万 5297 人	情報通信業	設定ミス
7	15 万 0165 人	卸売業，小売業	不正アクセス
8	12 万 0616 人	金融業，保険業	管理ミス
9	10 万 9112 人	情報通信業	不正アクセス
10	9 万 7438 人	情報通信業	不正アクセス

出典：NPO日本ネットワークセキュリティ協会
2013年 個人情報漏えいインシデントに関する調査報告書

個人情報漏洩事件・事故一覧

2015/10/20	メール本文に無関係のメールアドレスを誤記載 - 総務省
2015/10/19	2校分の生徒の個人情報含むUSBメモリを紛失 - 千葉市の中学校
2015/10/06	職員が住基台帳や課税台帳などデータ18万件を持出 - 西原村
2015/09/29	患者情報含むノートPCが院内で所在不明に - 平塚共済病院
2015/09/15	堺市の個人情報流出、あらたに561人分 - 有権者情報68万件の持ち出しも
2015/08/20	添乗員が参加者のパスポート写しを紛失 - 海外研修事業者
2015/08/05	居住者情報が保存された機器を誤廃棄 - 埼玉県内の郵便局
2015/07/30	シャトレーゼに不正アクセス - 会員情報21万件が流出か
2015/07/22	顧客情報含むファイルをメールへ誤添付 - 岡山の木工店

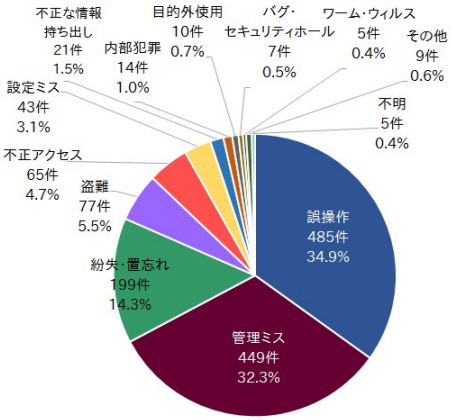
2013年 媒体・経路別漏えい件数



- 紙媒体による漏洩は2009年以降減少傾向
- 「インターネット」経由の漏洩原因では「不正アクセス」が約48%で最高
  パスワードリスト攻撃が増加したことが影響

出典：NPO日本ネットワークセキュリティ協会
2013年 個人情報漏えいインシデントに関する調査報告書

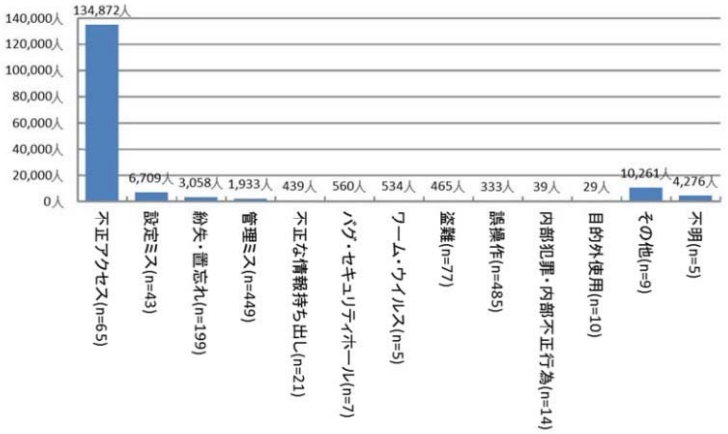
2013年 原因別漏えい件数



- 「誤操作」とは、メールやファックスの誤送信、紙媒体の誤配送といったヒューマンエラー。
- 「管理ミス」とは社内での紛失や誤廃棄

出典：NPO日本ネットワークセキュリティ協会
2013年 個人情報漏えいインシデントに関する調査報告書

2013年 原因別一件あたりの漏えい人数



出典：NPO日本ネットワークセキュリティ協会
2013年 個人情報漏えいインシデントに関する調査報告書

2013年 個人情報漏えいインシデント【概要】

漏えい人数	925万2305人
漏えい件数	1388件
想定損害賠償総額	1438億7184万円
一件当たりの平均漏えい人数	7031人
一件当たり平均想定損害賠償額	1億926万円
一人当たり平均想定損害賠償額	2万7701円

出典：NPO日本ネットワークセキュリティ協会
2013年 個人情報漏えいインシデントに関する調査報告書

個人情報の取扱いミスは信用毀損につながる

ソフトバンクモバイルが顧客の誤った情報を信用機関に登録

2013年10月に端末を割賦購入した契約者のうち6万3133件を「未入金者」として信用調査機関に誤登録。そのうち1万6827件についてはクレジット会社等から信用照会がなされており、信用審査に何らかの影響があった可能性があるという。

情報の誤りによる信用毀損で損害賠償の判決

破産宣告を受けた事実がないにもかかわらず信用情報センターが当人と名前が同じ他人の破産情報を間違って登録。これによりリース契約やローン契約が拒否されたため起業できなかったとして謝罪広告と損害賠償1100万円を求めた裁判。謝罪広告は認められなかったが220万円の損害賠償の支払いを命じた。（1990年5月判決）

社員の個人情報も当然に保護の対象

- ●会社案内や宣伝ページに無断で社員の顔写真を使ってないか　（社員だから勝手に写真を使っていいということにはならない。）
- ●必要以上の個人情報を掲載していないか
- ●退職済みの社員の情報が掲載されたままになっていないか
- ●不適切なネットワークモニタリングがなされていないか

職場等でのネット利用監視

事後モニタリング

監視カメラなどの流れを踏襲し、一定の要件の下で容認されていると考えられる。

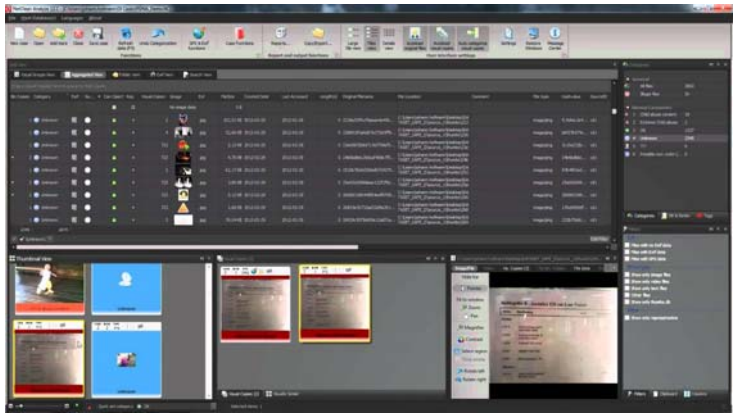
事前モニタリング

一般的には、以下のような場合、会社が従業員のネット利用を監視することは正当化されると解釈されるようである。

(1)会社側が業務を行うために必要である、または会社の所有物を保護するために必要な場合
(2)監視の方法が相当である
(3)監視について事前に従業員側の同意がある場合

企業が従業員のコンピューターをスキャン、児童ポルノは許されず

NetClean



1. 情報漏えいの原因と経路を知る
2. 情報奪取の攻撃方法を知る
3. スマホ・タブレットからの漏えいリスク
4. SNSのプライベート利用を甘く見ない
5. 情報漏えい対策６か条

標的型攻撃

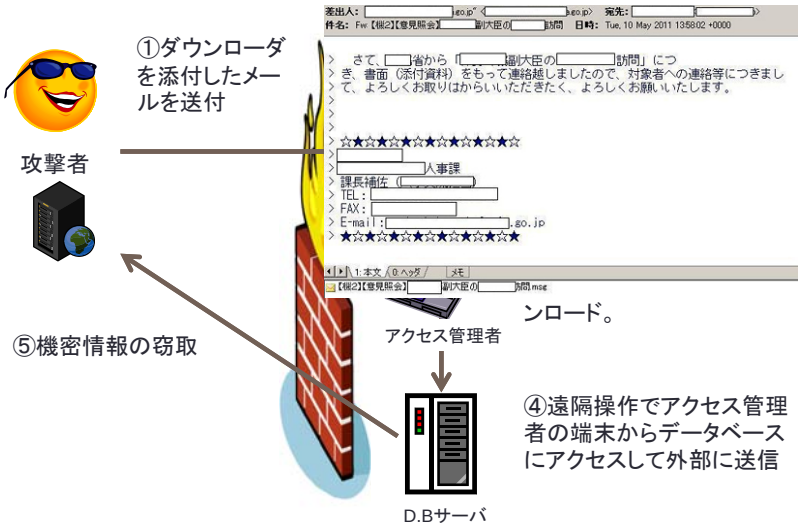
金銭や知的財産等の重要情報の不正な取得を目的として特定の標的に対して行われるサイバー攻撃。「プロの」犯罪者による財産犯的な性格。

使用される攻撃手法

ドライブ・バイ・ダウンロード、Microsoft SQL®インジェクション、マルウェア、スパイウェア、フィッシング、偽装メール

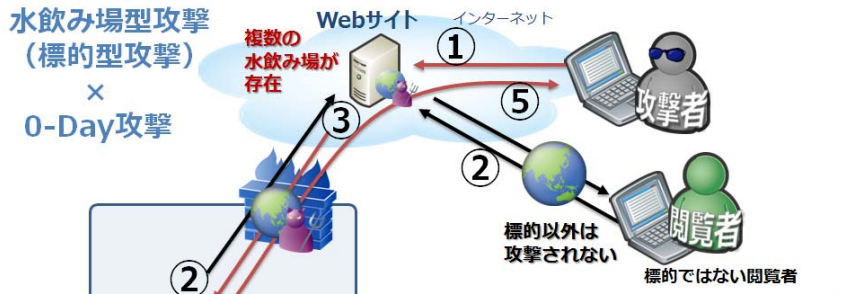
偽装メール＋不正プログラム ➡ **標的型メール攻撃**

標的型メール攻撃の一例



水飲み場型攻撃

水飲み場に集まる動物を狙う猛獣の攻撃になぞらえ、攻撃対象とするユーザーが普段アクセスするWebサイト（水飲み場）にコンピュータウイルスを埋め込み、サイトを閲覧しただけでコンピュータウイルスに感染するような罠を仕掛ける攻撃方法。



①攻撃者がWebサイトを改ざんし、不正なプログラムを設置

②いつも参照するWebサイトを閲覧

③特定の送信元IPからのアクセスに対してのみ
不正プログラムを配布（攻撃コードを返す）

④IE脆弱性を悪用したウイルス感染が成功

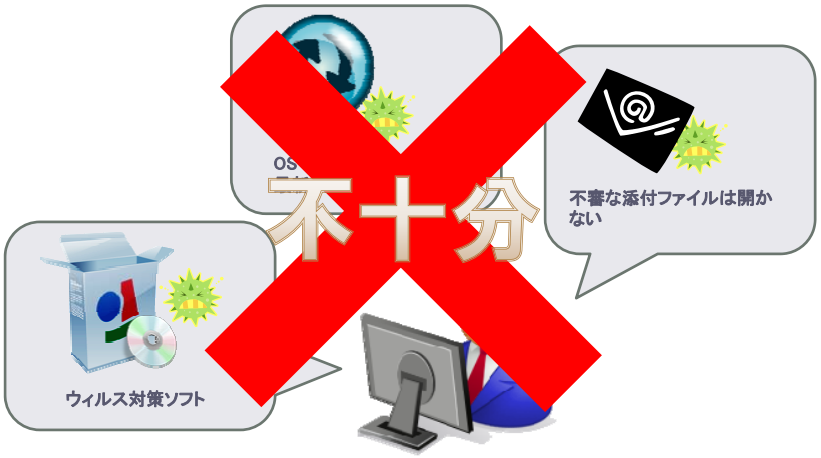
⑤攻撃者が用意したサーバへの通信が確立

出典：株式会社ラックの注意喚起情報より

遠隔操作型不正プログラムの脅威

画面の取得	遠隔操作	ウェブサイトへの書き込み
キーロガー	プログラム自身の消去	ウィルス対策ソフトに検知されない

遠隔操作ウィルス対策



不正遠隔制御対策ソフト

Optimal Guard概念図

盗難対策アプリ「ケルベロス」の悪用

逮捕の男　元交際女性の日常確認　666回録音

このようなアプリを無断で入れられることによる被害を防ぐには、タスクマネージャー系のアプリや「カンシチェッカー」などのアプリで動作を調べるのが有効。もし存在していたら、起動・ログインして管理者権限を無効にすればアンインストールできるようになる。

3つのレイヤから考えるスマホ・タブレットの漏えいリスク

ネットワークレイヤ

アプリレイヤ

OSレイヤ

ネットワークレイヤ

Free Wi-Fiスポットは通信傍受の危険あり

Wi-Fi自動接続を有効にしていると「なりすましホットスポット」に接続してしまう危険あり

アプリレイヤ

社用端末のルール

端末への機密データの保存を禁止する
端末外へのデータ転送、印字を禁止する
端末にデータを保存する場合は暗号化

アプリレイヤで無効化すべき機能

スクリーンショット
クリップボード履歴
USBケーブル接続によるデータ転送

二要素認証による不正ログイン防止

ID、パスワード+端末ID

OSレイヤ

マルウェアによる情報漏えい

OS不正改造や初期化による ルート権限奪取

iOS端末で構成プロファイル削除によるスクリーンショット保存

既存のソーシャルメディア利用のガイドラインについての所見

- ガイドラインを整備している企業や団体は多いが、あくまで業務上の利用を想定したもので、プライベートで利用する場合のルールまで定めたものはまだそれほど多くない。
- 業務で利用する場合とプライベートで利用する場合のルールが混同しているケースが見られる。
- 情報モラルに関する注意事項が中心で、情報セキュリティに関する注意喚起が欠けている

A社のソーシャルメディア利用についての留意事項

（役員・従業員向け）

個人情報や機密情報を公開しないようにしましょう

「A社個人情報保護方針」を遵守し、「個人情報取扱規程」で規定されている個人情報（社員情報、ユーザー情報や取引先の情報など）、また「情報取扱規程」で規定されている機密情報（開発情報や未発表の情報を含む）は、いかなる場合においても公開してはなりません。

個人がソーシャルメディアを利用する上でうっかり陥りがちなミスを事例で説明しておくとより効果的。

（例）取引先との出張の様子をSNSに公開する

余計な詮索をされる可能性があり、先方に迷惑をかけるおそれもあります。

利害関係人との行動は非公開が基本です。

（例）自分の行動を逐一SNSで公開する

A社に属していることを正しく伝えましょう

A社の役員・従業員が、個人で利用するソーシャルメディアのアカウント情報（例：プロフィール）には、A社に所属していることを正しく伝えるために、「A社に属していること」を明記することを推奨します。ただし、部署や組織名称は、非開示情報を含むことがあるため、記載しないようにしましょう。

名刺代わりに作るアカウントなら上記のとおりだが、純粋にプライベートで利用するアカウント情報には、勤務先などは書かないほうがよい。標的型攻撃のターゲットにされる危険性がある。

会社としての正式見解や回答では無いことを明示しましょう

ソーシャルメディアでの投稿は、個人としての投稿であり、会社としての正式な発言や見解、回答では無いことをアカウントの情報に明記しましょう。さらに、A社や、A社に関する発言を行う場合、その個々の発言において「個人の意見であり、会社としての正式な発言や見解、回答では無い」旨を示しましょう。万一、発言によってA社が不利益を被った場合、損害賠償請求の対象になることもあります。

純粋にプライベートで使用するアカウントでは、「たとえ個人的見解だとしても組織の運営や方針に対する不用意な発言は慎むよこと」としておくほうがよい。

ソーシャルメディア利用のガイドライン（プライベート編）のモデル構成

1.ガイドラインの目的

2.ソーシャルメディアの定義

3.適用範囲

4.遵守事項

5.禁止事項

附則
平成26年○月○日施行

ソーシャルメディア利用のガイドライン（プライベート編）のサンプル

遵守事項

（1）常に誠実で良識ある発言・投稿を心がける
ソーシャルメディアの利用に当たっては個人の発言の自由、思想の自由を尊重しますが、情報を発信する場合には、当社従業員としての自覚と責任を認識し、常に誠実で良識ある発言・投稿を心がけましょう。

（2）法令・規律・行動規範の遵守
ソーシャルメディア利用の場面においても各種法令、就業規則の服務規律及び職員行動規範を遵守しましょう。
個人が特定できる写真や映像、文章などを投稿する場合は事前に本人や所属団体、企業などに了解を得るなど、肖像権、プライバシー権、著作権などに十分留意しましょう。

遵守事項

（3）仕事にまつわる発言・投稿をする際は内容に十分注意する
ソーシャルメディアのプロフィール上で当社に所属していることを明記している場合はもちろん、たとえ明記していなくても、同僚や上司、更にあなたの職場を知る知人もそれらのコンテンツにアクセスしたり、転送されて目にしたりする場合があります。そのため、発言する内容は、あくまであなた個人の見解や意見であり、組織の見解や意見を代弁するものではないことを明確にしてください。なお、組織の公式見解や利益に反する投稿を行った場合は、組織のイメージ毀損につながる議論や憶測を引き起こす可能性があることを認識し、内容に十分注意しましょう。

（4） 会社に関する否定的な投稿への対応は組織に任せ、自分の判断で行わない
当社に関する否定的な投稿を見つけて、その中に事実誤認が含まれていたとしても、個人の判断で否定や反論をすることは避け、所属長まで速やかに連絡して組織としての対応に委ねましょう。

遵守事項

（５）アカウント乗っ取り、情報詐取の手口に十分注意する
異なるソーシャルメディアで同じID、パスワードを使用していると、一箇所から情報が漏えいした場合にすべてのサイトのアカウントが乗っ取られる危険性があります。 ID、パスワードはサイト別に管理するようにしましょう。
ソーシャルメディア上に投稿された記事や広告の中には、攻撃サイトへ誘導するものや、悪意のプログラムが仕掛けられたアプリをダウンロードさせるものがあります。ダウンロードしようとするアプリが信頼のおけるものかどうかよく確認するようにしましょう。
リンク先ページがソーシャルメディアサイトへのログイン認証を求めてくる場合は、ID、パスワードを騙し取ろうとする偽サイトの可能性があります。ログインページが正規のものかを必ず確認するようにしましょう。

禁止事項

（１）秘密情報を含む発言・投稿をしないこと
個人的な見解を述べる場合でも、業務上知り得た非公開情報や当社のセキュリティを脅かすおそれのある情報（以後、秘密情報という）を含む発言・投稿を行うことは一切禁止します。秘密情報かどうか確信が持てない場合は、発信する前に所属長に相談するか、その話題について言及することを控えてください。噂や未発表の事柄について尋ねられた場合も同様とします。

（２）違法性のあるコンテンツ、誹謗・中傷を含む発言・投稿をしないこと
次に掲げる発言・投稿をしてはなりません。
- ●人種、思想、信条などの差別、または差別を助長させる情報
- ●違法情報または違法行為を助長する情報
- ●その他公序良俗に反する一切の情報

禁止事項

（３）就業時間中の発言・投稿をしないこと
職員には職務に専念する義務が課されているので、業務として利用する場合を除き、就業時間中（休憩時間中は除く）の発言・投稿は慎むこと。ソーシャルメディアに公開した情報は、同僚や上司、更にあなたの職場を知る知人もそれらのコンテンツにアクセスしたり、転送されて目にしたりする場合があることを忘れず、節度ある利用を行うようにしましょう。

情報漏えい対策6か条

1. 業務に必要な通信機器は貸与せよ
2. FAX、メールは誤送信対策を
3. ネットワークの二重化
4. 外部記憶媒体の制限
5. 退職後の職員のアカウント処理
6. 廃棄方法のルール

1 業務に必要な通信機器は貸与せよ

（理由）

1. **個人所有機器を使わせるとセキュリティ管理も個人まかせになる**

2. **刑事責任に問えなくなる可能性があるため**

※日本には情報窃盗罪がないので、個人所有の機材に情報をコピーされて持ち出された場合には、窃盗罪は成立しない。

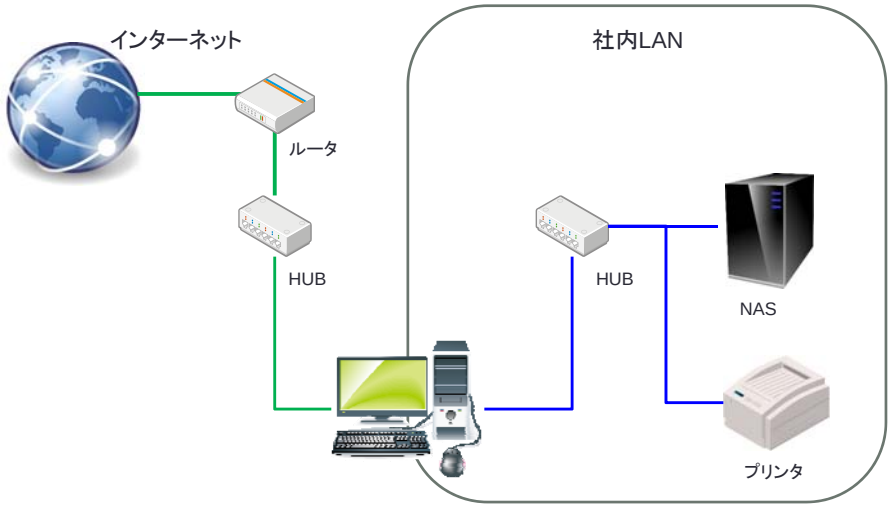
どうしても個人のモバイル機器を業務で使用せざるを得ないなら、「エンタープライズ・モビリティ管理（EMM）」を導入する

2 FAX、メールは誤送信防止策をとる

FAX で番号を間違えた場合、その番号がたまたまFAX 回線であれば、そのまま相手先に届いてしまう。
また、アドレス帳からの選択を間違えると、有効なメールアドレスなので、そのまま別人に届いてしまう。

- FAXのテスト送信
- メール送信ディレイの活用

3 ネットワークの二重化



4 外部記憶媒体の制限

外部記憶媒体への書込み制限

指定した端末以外ではCD/DVDの書き込みができないようにするなど

USBポートの使用制限

指定したUSBデバイス以外の接続を禁止し、私物のUSBメモリ等を使用した情報の持ち出しを防止するなど

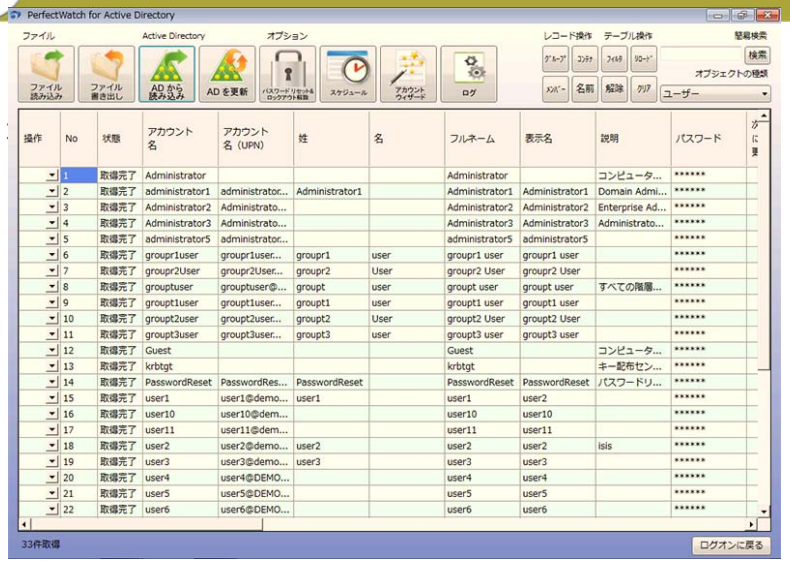
備品のUSBメモリ等の管理

管理台帳を作成してUSBメモリの使用者、返却日を記録するなど

機密データの社外持ち出しルール

データを社外に持ち出す際は上司の承認を必要とする、持ち出すデータは暗号化するなど

5 退職後の職員のアカウント処理



6 廃棄方法のルール

紙媒体の廃棄

機密情報が印字された紙媒体を廃棄する際は、シュレッダーを使用すること。

機密情報が印字された紙媒体を社外へ持ち出すことは原則禁止する。やむを得ず持ち出す場合は、事前に所属長の承認を必要とする。

使わなくなったPCの廃棄

HDDを物理的に破壊する

専用ソフトを使って論理的にデータを完全消去する

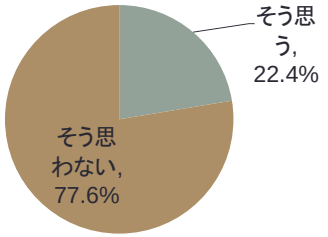
専用装置を使って強磁気でデータを完全消去する

↳ 壊れて、ハードディスクのデータ消去作業ができないPCでも対応可能

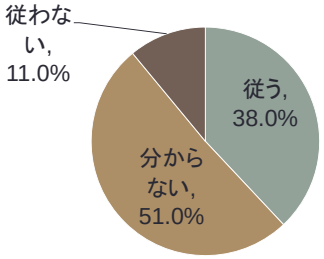
おわりに

組織の風土としてモラルが確立されていないと個人のモラル向上は期待できない

従来の基準や慣習には反しても、法律に反しないことであれば、どんな強引な手段や方法をとっても問題はない

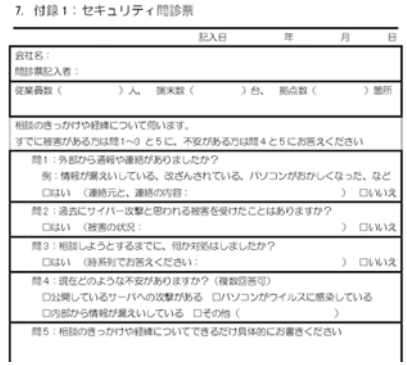


上司から、会社のためにはなるが自分の良心に反する手段で仕事を進めるように指示されましたときあなたは・・・



出典：公益財団法人日本生産性本部「2013年度　新入社員　春の意識調査」

「やられたかな？」と思ったら、専門家へ相談する前にやることがある



7. 付録１：セキュリティ問診票

記入日　　年　　月　　日

会社名：
問診票記入者：

従業員数（　　）人、　端末数（　　）台、　拠点数（　　）箇所

相談のきっかけや経緯について伺います。
すでに被害がある方は問1～3 と５に、不安がある方は問４と５にお答えください

問１：外部から通報や連絡がありましたか？
例：情報が漏えいしている、改ざんされている、パソコンがおかしくなった、など
□はい　（連絡元と、連絡の内容：　　）　□いいえ

問２：過去にサイバー攻撃と思われる被害を受けたことはありますか？
□はい　（被害の状況：　　）　□いいえ

問３：相談しようとするまでに、何か対処はしましたか？
□はい　（時系列でお答えください：　　）　□いいえ

問４：現在どのような不安がありますか？（複数回答可）
□公開しているサーバへの攻撃がある　□パソコンがウイルスに感染している
□内部から情報が漏えいしている　□その他（　　）

問５：相談のきっかけや経緯についてできるだけ具体的にお書きください

日本セキュリティオペレーション事業者協議会（ISOG-J）
「やられたかな？その前に」ガイド～『やられてる！』と思ったら～
http://isog-j.org/output/2015/Yararetakana-Guide-20151014.pdf

END