

「違反すると会社でパソコンが使えない 大塚商会のセキュリティへの取り組みと IT活用のご紹介」

2008年12月17日(水)

Network security Forum 2008

株式会社大塚商会 トータル情報システム室

執行役員 中野 清

大塚商会とは

トータル&ワンストップソリューションプロバイダとしての総合力で、
お客様が直面するさまざまな課題を解決します。

配
コスト削減
オフィスサプライ等の手



業務効率UP!
文書データ化と省スペース
化

スクールに参加するの
もいいが、独自の社員教育
を行いたい。

内部統制!
堅牢なセキュリティの
ネットワーク構築

事業領域

SYSTEM INTEGRATION

(システムインテグレーション事業)

コンサルティング

業務改革コンサルティング
内部統制構築支援コンサルティング
セキュリティコンサルティング
現状調査分析コンサルティング
SI導入支援コンサルティング

ソリューション

ERP／業種・業務
CAD(建設・製造・解析)
企業内情報システム
文書管理／データ活用
セキュリティ
OS／データベース
IT機器／OA機器販売
回線／通信ネットワーク

SERVICE & SUPPORT

(サービス&サポート事業)

アフターサポート
インターネットサービス
セキュリティサービス
データ復旧
データ消去&パソコン買取サービス
教育支援
アウトソーシング



オフィスサプライ用品の通信販売
購買・調達サービス



マルチベンダ

マルチフィールド

施設・拠点・就労者数

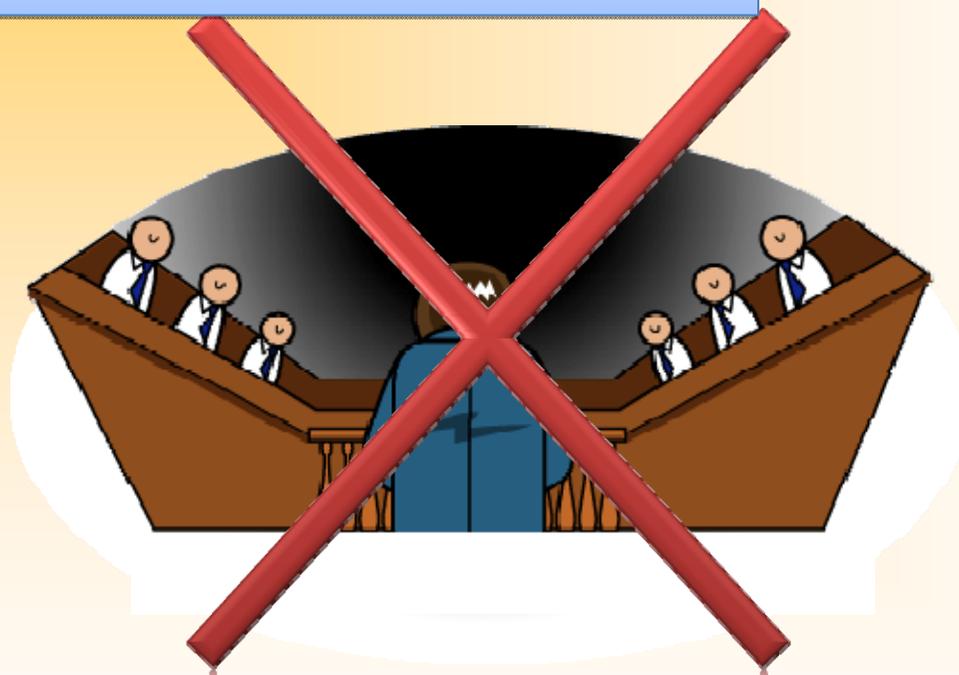
全国約270店課

IDC: 4センター(市川・渋谷・秋葉原・関西)
ODTセンター : 1センター(東京)
CTOセンター : 2センター(東京、大阪)
コールセンター : 2センター

就労者数は正社員・派遣・アルバイト込みで約7400名(業務委託者除く)

「罪人を作らない」という方針

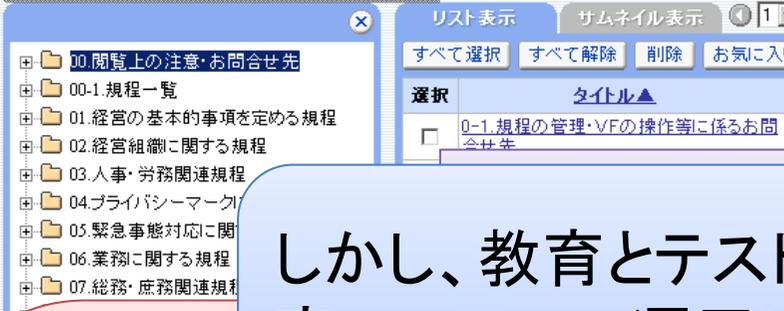
- ・会社は事故が発生しにくいシステムと運用の構築
- ・就労者はルールに則った業務を行う



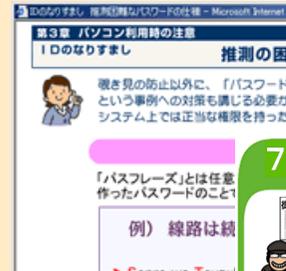
万が一、ルールに則ったプロセスで事故が発生したとしても、その責任は会社であり、個人の責は問わないという考え方

社内ルールの案内と教育

大塚商会規程集



Webラーニングを使った研修とテスト



7 車両管理の徹底・無線LANの無効化



しかし、教育とテストを行って、すぐに就労者が高いモラルで運用にたずさわれるとは考えられなかった...

特にセキュリティルールは...
て、メール...
→いつでも参照可能に



	職位	対象人数	完了者	完了率
1	役員	39	23	59%
2	部次長	132	83	63%
3	課長	1,001	799	80%
4	係長	1,183	97	8%
		1,724	1,017	59%

受講進捗を役員会で配布
→役員・部長の受講が促進し、全就労者への運用徹底につながった

CP免許制度の導入へ



- 運転免許証からヒントを得た、
研修の進捗や運用の徹底度合い、免許を取る
がひと目でわかる制度を作ろう！ 度

社員証がない
に入れない！



CP免許がないとパソコン
が使えない！

CP免許の種類



1級：定められた規程に関してコンサルティング・構築ができる。



2級：定められた規程の改善・追加の提案ができる。



3級：定められた規程を実践し人に指導ができる。



4級：定められた規程の理解ができる。

CP免許の減点テーブル抜粋

規程名	規程違反種別	減点数	所管部署
情報システムセキュリティ規程	情報システムセキュリティ規程違反	1～10	トータル情報システム室
	コンピューターウイルス対策基準違反	1	トータル情報システム室
	WindowsUpdate未実施	1	トータル情報システム室
	ネットワーク作業注意義務違反	1～6	トータル情報システム室
	ウイルス感染	1～6	トータル情報システム室

「情報セキュリティ規程」「機密管理規程」「個人情報保護規程」に違反すると減点

ルール徹底への取り組みとして

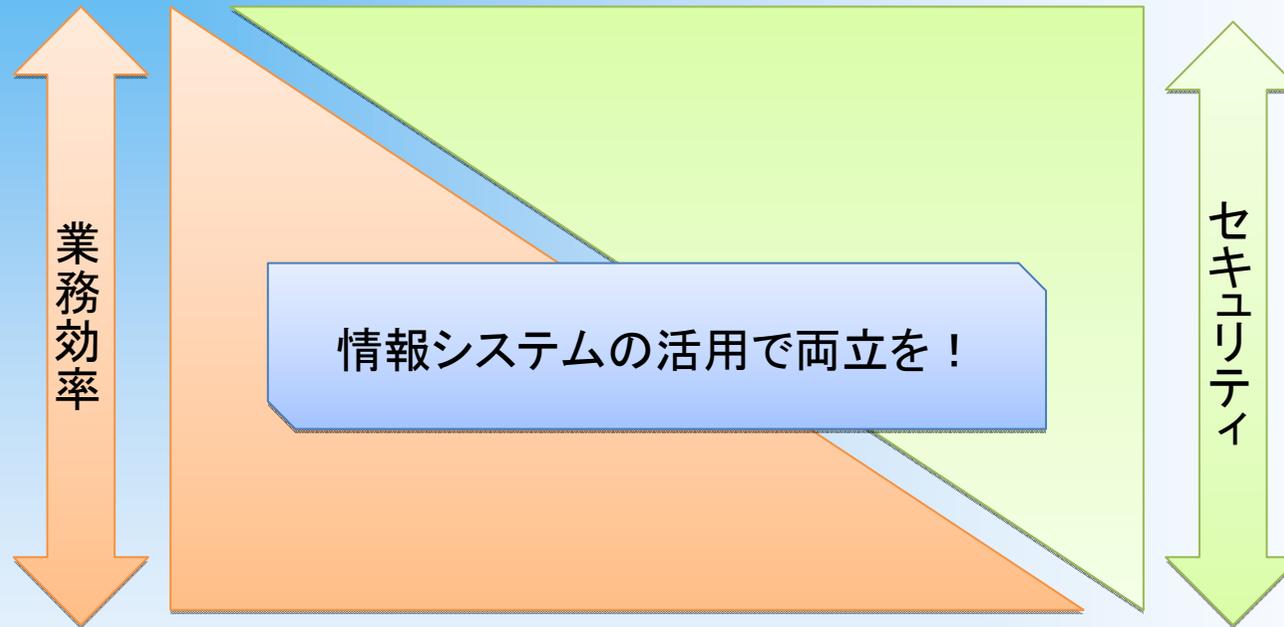
- このCP免許を就労者のセキュリティ意識向上ツールとしていく計画



経済産業省ホームページ

「V. 事業者ごとの個人情報保護対策取組事例」に当社が紹介されています。

業務効率アップとセキュリティ



- セキュリティ上問題があるからと言って機材やデータの利用を禁止しては、ユーザ対応に支障が...

携帯・スマートフォンのセキュリティ

社内でしかできなかった作業を社外からも可能に！



端末紛失対策(社員は常にカード持参)→
連絡により工場出荷状態に戻す仕組み

スマートフォン・PHS・携帯電話紛失時の連絡先
(24時間365日対応)

ソフトバンク	ウィルコム	ドコモ
0120-***-***	0120-***-***	0120-***-***

※ドコモ携帯電話を紛失した場合は、上記に連絡する前に遠隔操作で携帯端末のロックを行ってください。

※ドコモ携帯電話の契約者住所(大塚商会本社)
東京都千代田区板田橋2-18-4 TEL 03-3264-7111

自分の携帯番号	***-***
---------	---------

- 社が指定したセキュリティ対策を実行していれば、紛失しても機密データは流出しない

Point!

株式会社大塚商会

社内標準環境と監視(ハード・ソフト)

持ち運びが難しいデスクトップPCに、標準ソフトをインストールして配布

監視ソフト導入



ソフト・ハードは専用システムで購入から廃棄まで一元管理
購入申請は情報システム室長の統一した承認処理

- 未許可機器接続、未許可ソフトをインストールした場合、セキュリティ義務違反としてペナルティ



株式会社大塚商会

ノートPCのセキュリティ

このパスワードを忘れるとシステムが起動しない

パワーオンパスワード入力

【モバイルコネクト パスワード初期設定】

<入力画面>

登録したい位置の数字を入力してください。

8	4	9	0	☀	6	7	2	5	☘	3	1	5	1
7	8	2	6	☎	9	0	3	4	☞	3	4	8	7
9	2	5	0	🔍	6	1	1	0	🚗	4	6	8	9
3	7	5	2	☕	7	5	3	2	👤	0	4	8	1

[for 顧客コード: [] ユーザID: []]

Serviced by
Mobile Connect
(Japan)

1. パワーオンパスワード
2. USBキーロック
3. Windowsログオンパスワード
4. 社内イントラへの接続時のワンタイムパスワード
／社内システムへのログオンパスワード
5. 万データを持ち出す場合は暗号化
 - ・ セキュリティ設定に違反した場合はペナルティ

キーがないとスクリーンセイバーが起動して解除できない



株式会社大塚商会

便利で危険なUSBメモリ

電子機器持出管理システム

いつ・誰が・何の目的で使っているか
利用状況の監視・管理

電子機器持出状況検索

検索条件
 ・持出予定日時 2008 年 1 月 28 日 16
 ・電子機器種別 全て

該当件数3件

申請番号	電子機器種別	識別名	機材管理番号	機材管理
233-37	USBメモリ	S10001		15
	USBメモリ	S10001		15 持出可
	USBメモリ	S10002		

終了

データ交換に便利なUSBメモリは
社内使用禁止でした

検索条件
 ・ステータス 持出中
 ・電子機器種別 全て
 ・識別名 (前方一致)
 ・機材管理番号 (前方一致)
 ・申請社員コード (完全一致)
 ・申請社員名 (前方一致)

28件

持出申請日 返却申請日	ステータス	識別名	電子機器種別 機材管理番号	申請者 社員コード 社員名	承認者 社員コード 社員名	配布先部署名	持出予定日時
2007/12/15	持出中	S20062	USBメモリ H0B000022	12345 大塚 太郎	1234 田中 虎平	ASC SPCル-プ ホ	2007/12/15 19:00
2008/01/09	持出中	S30113	USBメモリ H0B000000	1234 大塚 一郎	12 山田 太郎	LA技術カル-プ A	2008/01/09 17:00
2007/12/28	持出中	S30112	USBメモリ H0B000099	1245 大塚 太郎	12 山田 太郎	LA技術カル-プ A	2007/12/28 16:00
2007/12/25	持出中	S10228	USBメモリ H0B000006	125 大塚 花子	145 鈴木 太郎	関西技術カル- プCA	2007/12/25 11:00

今時USBメモリが
ないとユーザー対
応できません！



- USBメモリは課単位
で必要最低限配布し、
所属長が嚴重管理

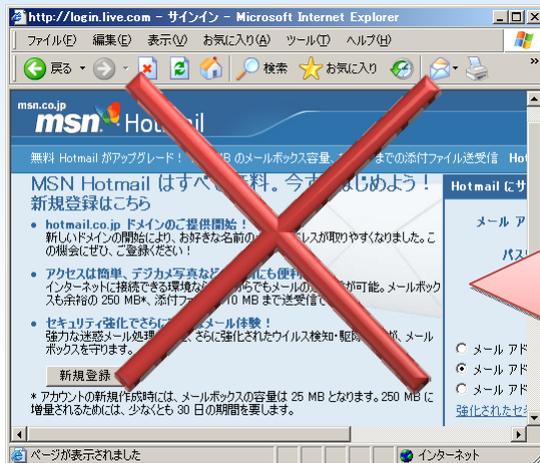
電子メールのリスク対策

メール監査システム導入



自社ドメイン以外のアドレス送信ブロック→
他社へのウイルス感染防止対策／私用メール対策

誤操作対策として、
一度に100通以上メール配信ブロック

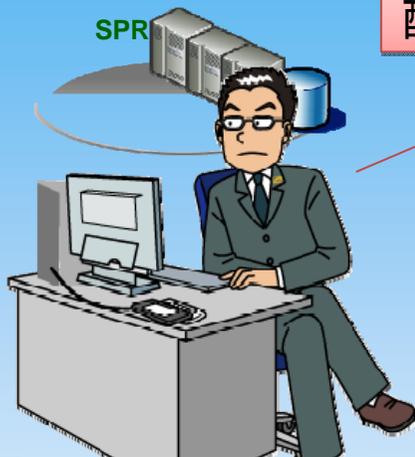


URLフィルタリングによるWEBメール利用ブロック

メール・DMの配送一括管理

各店課からの
配信・発送は禁止

メール配信・DM発送は、電子承認
システムでの依頼に統一

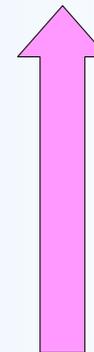
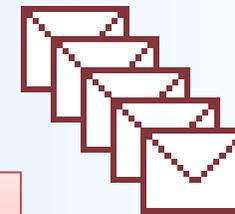


各課担当者



承認部署

「配信不要リスト」と照合した上で、送信を実行



DM関連専門部署

株式会社大塚商会

木曜日のセキュリティチェックイベント

大塚商会ポータルサイト(OtsukaPortal)

TSUKA PORTAL

大塚商会ポータルサイト(OtsukaPortal) 全社への通達・連絡 各部門内の通達・連絡 組

ミッションステートメント

重要
申請
検索
会議室予約
リンク集
就労者照会
勤務管理
ガイド(Q&A)
グループウェア
教育MYページ

大塚商会ポータルサイト(OtsukaPortal)

平成20年度...

「お客 **本日WindowsUpdateDay**

通達事項(伝) **本日WindowsUpdateDay**

緊急WindowsUpdate

08/11/06

08/10/30

08/11/13

本日ウイルスチェックデー

緊急WindowsUpdate

緊急ウイルスチェック

ウイルス侵入
怪しいメールの添付ファイルは
開かないでください

ウイルス対応のため
メールサーバーを停止します
詳細は右記を参照してください

- ウイルスチェック未実施、Update未実施はセキュリティ義務違反としてペナルティ



公開サイトチェック



チェック項目

1. 最新のセキュリティパッチの適用
2. ファイアウォールは必要最低限のアクセスのみを許可
3. フォルダへのアクセス権に問題ないか
4. 必要でないサービスが稼動していないか
5. 公開サイト上(サーバのディスク上)に見覚えのないファイルが存在していないか
6. クロスサイトスクリプティング対策は実施済みか
7. SQLインジェクション対策は実施済みか
8. 脆弱性のあるスクリプトマッピングを削除
9. アクセスログ

事故状況の即時把握 継続的改善