

第9回 情報セキュリティ EXPO に出展いたします 弊社ブースに是非お立寄り下さい。

拝啓 貴社益々ご清栄のこととお慶び申し上げます。平素は格別のご高配に賜り厚く御礼申し上げます。

さて、弊社は、来る5月9日(水)～11日(金)東京ビッグサイトにおきまして開催されます、「第9回 情報セキュリティ EXPO」に出展する運びとなりましたので、ここにご案内申し上げます。

情報セキュリティ EXPO は、情報セキュリティ対策のあらゆる製品が一堂に集まる専門展です。弊社では、昨今のサイバー攻撃からのセキュリティ対策として Web アプリケーションファイアウォール「WAPPLES(ワップル)」、WAPPLES を搭載したセキュアな Web サイト環境を低価格で実現する「WAF 付きクラウドサービス」、内部情報漏洩対策としての DB 暗号化「D'Amo」、更に BCP 対策として遠隔バックアップサービス「用心坊」を出展させていただきます。

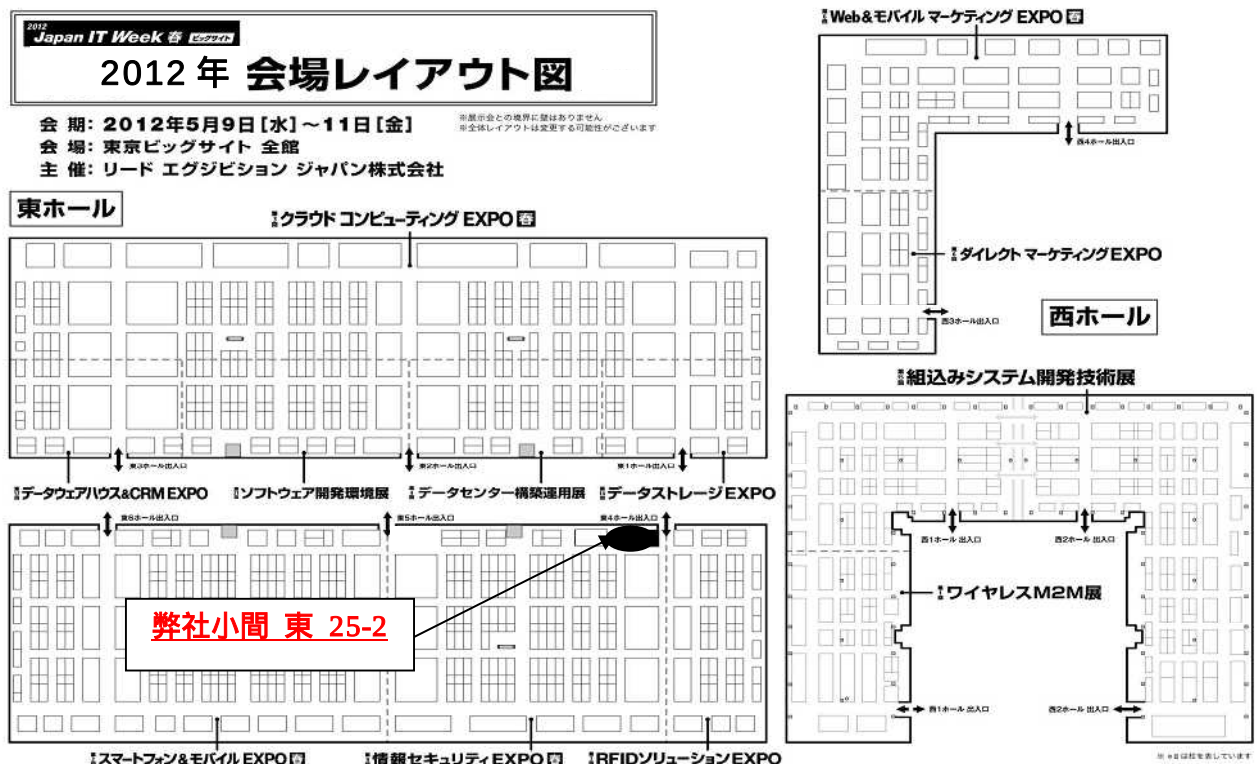
弊社の小間番号は東 25-2にて出展いたしますので、ご多忙中、大変恐縮ながら是非この機会にご来場賜りますようお願い申し上げます。

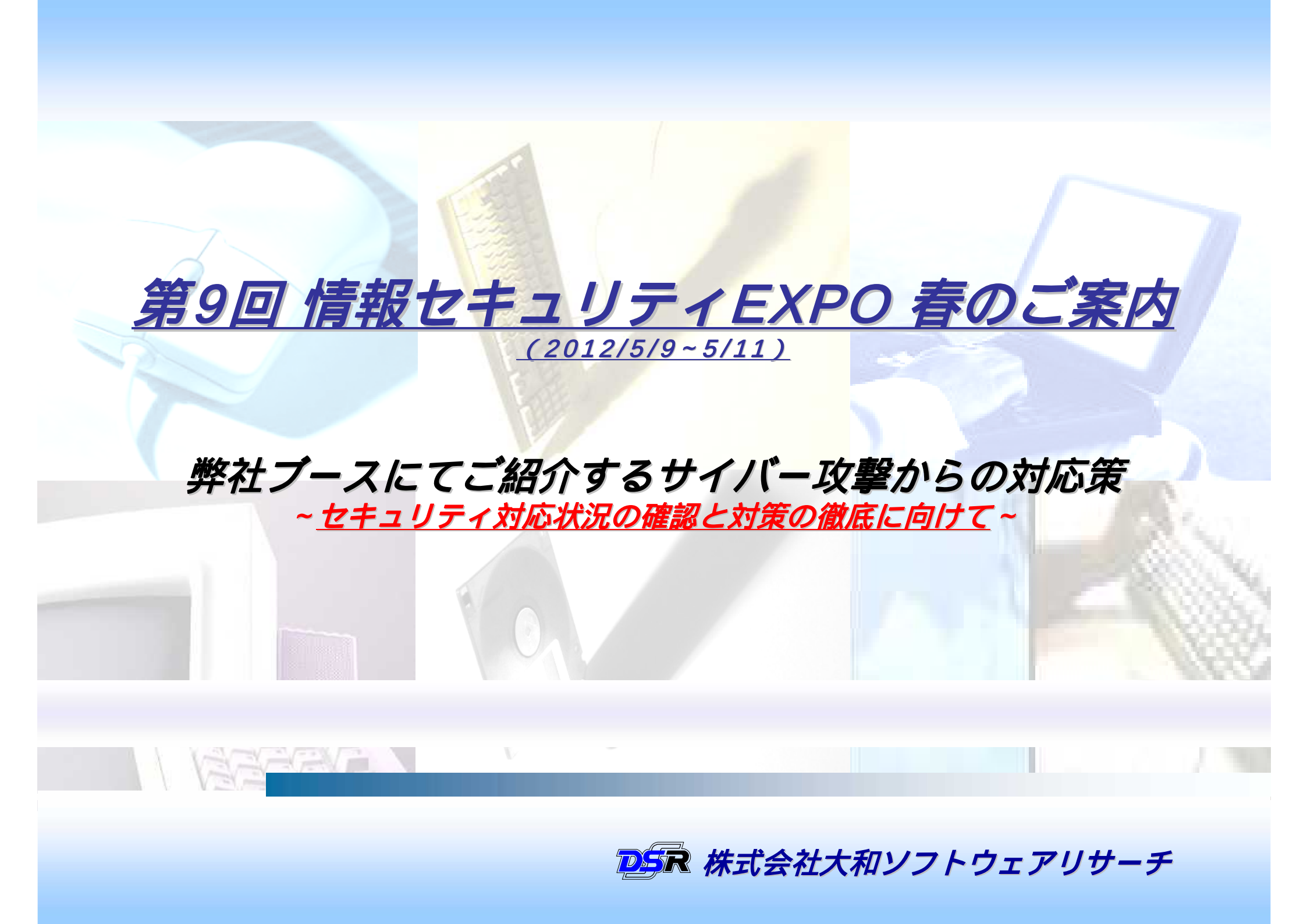
また、当日は同封の招待券を必ずお持ち下さい。(追加の招待券が必要な場合は、弊社まで連絡下さい。至急送付させていただきます。)なお、本券をお持ちいただかない場合は有料(¥5,000)となりますのでご注意下さい。

貴殿のご来場心よりお待ちしております。

敬具

(株)大和ソフトウェアリサーチ
代表取締役社長 竹末 圭五





第9回 情報セキュリティEXPO 春のご案内

(2012/5/9 ~ 5/11)

弊社ブースにてご紹介するサイバー攻撃からの対応策
~ セキュリティ対応状況の確認と対策の徹底に向けて ~

脅威を増す標的型のサイバー攻撃に関する注意喚起

昨年発覚したStuxnetによる攻撃に続いて、今年に入って海外では、航空機メーカーへの攻撃やインターネットを介した大量の個人情報漏洩事件などが発生し、9月19日には、国内で大手総合重機メーカーへのサイバー攻撃が報道されました。

今回の大手総合重機メーカーの事件は標的型の攻撃であり、初めに業界団体に侵入(感染)し、その団体のメールを窃取、そのメールを悪用してウイルスファイルの傘下の事業者に送りつけ、目的の事業者への侵入を図っていたとのこと。

従って、自組織のセキュリティ面で弱い所を如何に無くすかが、一組織だけでなく業界としての喫緊の課題となっております。組織のシステム管理者は下記の対策を踏まえ、不正アクセスや侵入、ウイルス感染の検知や防御策を検討し、日頃からの対策を徹底することが必要です。

(1) 取り扱う組織情報の重要度、機密度を精査する

(2) 企業の社会的責任と事業継続性の観点から、相応の対策を選択することが重要

(3) グループ企業や連携している組織では、統制されたポリシーと対策が必要

脅威を増す標的型のサイバー攻撃に関する注意喚起・・・より一部抜粋（平成23年10月：IPA【独立情報処理推進機構】）

1. サイバー攻撃からの対応策

企業(組織)における対策の基本的な観点

IPAからの呼びかけ：8つの対応策

対策(1)

入口(ネットワーク経路)をしっかり守る

技術的な対策事項

システムへの入り口と経路での防御

対策(2)

ファイアウォールを抜けてもシステムにつけ入れられる隙(脆弱性)を与えない

脆弱性対策

対策(3)

標的型攻撃のルートとなる箇所を防御する

標的型攻撃ルート対策

対策(4)

ウイルスの活動(組織内蔓延や外部通信)を阻害、抑止する<出口>

ウイルス活動の阻害および抑止
(出口対策)

対策(5)

重要な情報はその利用を制限(アクセス制御)する

アクセス制御

対策(6)

情報にアクセスされても保護するための鍵(暗号)をかける

情報の暗号化

対策(7)

操作や動き(ログ証跡)を監視・分析し不審な行為を早期に発見する

システム監視、ログ分析

対策(8)

万一被害が発生したら早急な対応(ポリシーと体制)をとる

管理統制およびコンテンジェンシープラン
(事前準備・事後対応)

前／後方でのセキュリティ対策がポイント

今すぐ実現できるセキュリティソリューション < DSR から提供可能なサービス >

業務を支えるICTインフラへのサイバー攻撃対策

脆弱性対策

インターネットからファイアウォールを抜けて、
WEBサイトへ仕掛ける不正アクセス攻撃を検知 / 防御
入口 / 出口: 情報漏洩対策

WAPPLES (WAF 製品)

**Webサイトの個人情報漏洩・不正
アクセス対策は万全ですか？**

WAF (Webアプリケーションファイアウォール)



- Webサイト攻撃に対する
検知・防御
- 個人情報漏洩対策
- ハッカーから安全に
情報を保護

情報の暗号化

重要な情報 (DB) にアクセスされても保護するため、
鍵 (暗号) をかける
内部の情報漏洩も防御

D Amo (DB暗号化)

DBセキュリティ対策が急がれています！



データベース暗号化セキュリティソリューション

- 暗号: DB内のデータをカラム単位で選択して暗号
- アクセスコントロール: DB全体または暗号化
カラムへのアクセスコントロール
- 監査: 監査ログ取得可能

当日は、担当者より詳細説明、デモおよびセッションによる製品紹介をご用意しております！！

利便性そして、安全性を重視したデータセンター

都心のハイセキュアなデータセンターである@Tokyo(アット東京)内のロケーションにて、災害対策はもちろんのこと計画停電も考慮した自家発電装置設備などBCP:事業継続支援に万全なソリューションをご用意いたしました。
ハウジングサービス、遠隔バックアップサービス、Webサイトへのセキュリティ対策を考慮したクラウドサービスなど、スケーラビリティの広いアウトソーシングサービスをご提供いたします。

セリング ポイント



- 堅牢な設備環境【免震/耐震構造、安定性の高い電源系統、信頼性の高いインターネット接続サービス】
 - ☞ 東京センターのフロアには更に自家発電装置も付いている為、災害対策はもちろんのこと、計画停電対策等の経営課題に対応する、万全な環境をご提供致します！
- 統合監視環境により、ハウジング機器のトータルマネジメントサービスを実現
 - ☞ システム監視、サーバ監視等による迅速なダウン対策、予防保守・改善が可能です！
- 都市型IDCとしての好アクセス条件
 - ☞ 都心からの交通の便も良いことから、HW等の障害時において駆けつけが容易です！

データセンター概要

◆ システムサービスセンター概要

- 総床面積 14万㎡の世界最大級データセンター
- 震度7にも耐えうる堅牢なファシリティ
- 電源系統の多重化を含む高信頼度の電源供給
- 最新の技術を活用した24時間365日の監視システム
- 高速・大容量のインターネット環境

@Tokyo



◆ 最高レベルのセキュリティー



セキュリティゲート

◆ あらゆるニーズに対応する サーバスペース



拡張性の高いサーバールーム

◆ 堅牢なファシリティと 高信頼度の電源供給



免震構造の採用



最高レベルの技術・ノウハウによるセキュリティ



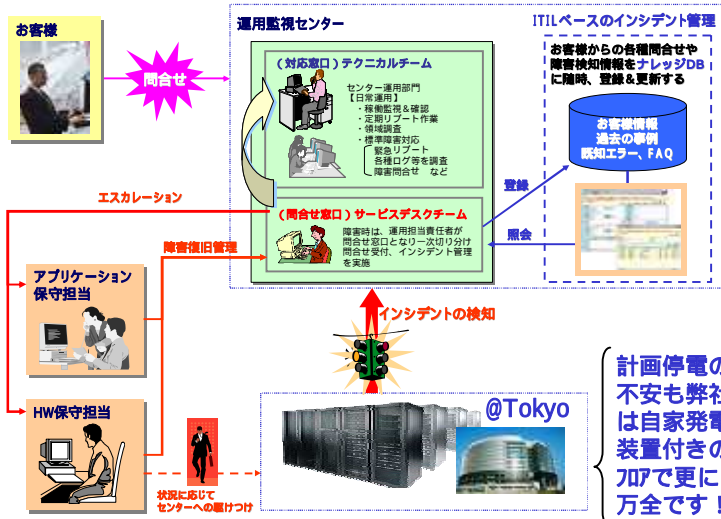
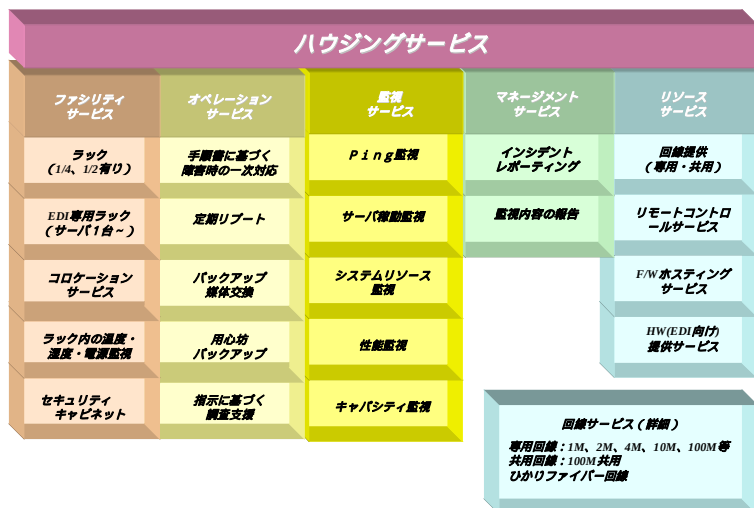
サーバールーム内観



高信頼度の電源をご提供

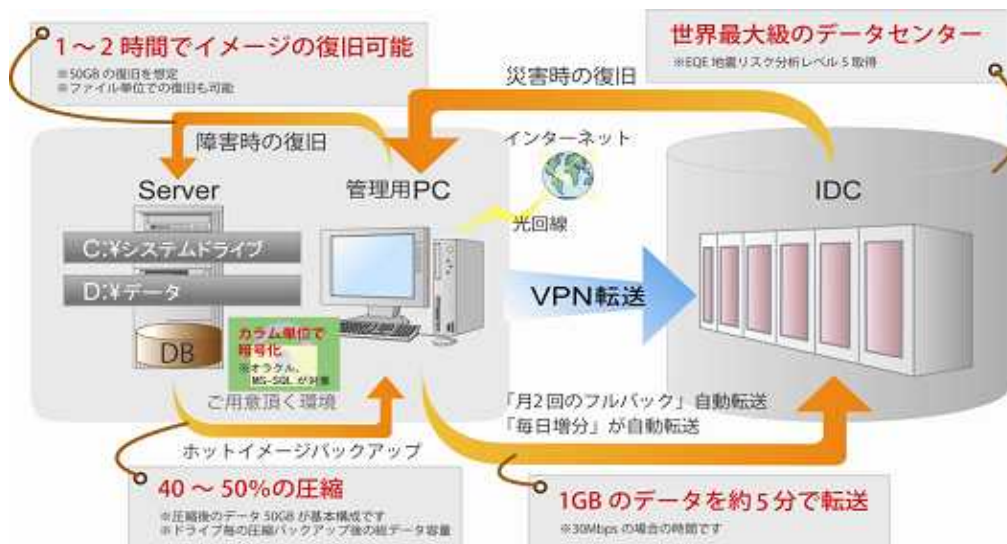
BCP支援 :ハウジング'サービス

災害/計画停電に影響を受けないIDCに移設！



BCP支援 :遠隔'バックアップ'(用心坊)

(¥69,800 ~ /月)のサービス提供です！！

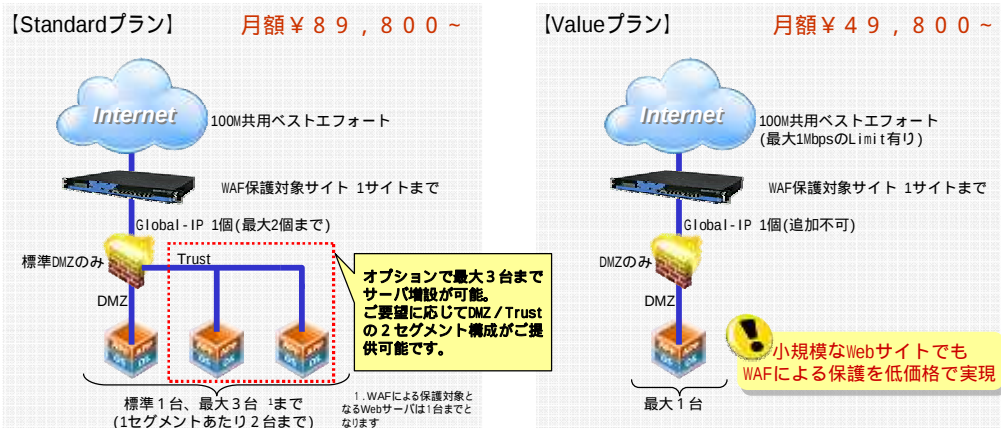


今やるべき**災害対策**とは…**遠隔地へのバックアップ**です！！

用心坊とは、企業の重要なデータの**障害対策、災害対策、セキュリティ対策**をひとつにまとめ、更にそれらの作業を**自動的に**行うことのできる**業界最安値 (¥69,800 ~ /月)**の遠隔バックアップサービスです。しかも単なるファイルだけでなく、**イメージバックアップ方式**を採用しているので復旧が迅速です！

BCP対策 :WAF付きクラウド'サービス

クラウドの選択はWebサイトのセキュリティ対策です！



下記のWebサイトに対する**攻撃パターン**について、**検知/防御**が可能となります！！

1	Buffer Overflow	14	Privacy File Filtering
2	Cookie Poisoning	15	Privacy Input Filtering
3	Cross Site Scripting	16	Privacy Output Filtering
4	Directory Listing	17	Request Header Filtering
5	Error Handling	18	Request Method Filtering
6	Extension Filtering	19	Response Header Filtering
7	File Upload	20	SQL Injection
8	Include Injection	21	Stealth Commanding
9	Input Content Filtering	22	Suspicious Access
10	Invalid HTTP	23	Unicode Directory Traversal
11	IP URI	24	Web Site Defacement
12	IP Filtering	25	URI Access Control
13	Parameter Tampering	26	User Defined

ご連絡先



株式会社大和ソフトウェアリサーチ
〒102-0083
東京都千代田区麹町1-5-2
アウトソーシングソリューション部
TEL:03-3262-8558 FAX:03-3262-8867

URL <http://www.dsr.co.jp>

