

内部統制に向けた リスクマネジメントサービス

2007年2月7日

(株)NTTPCコミュニケーションズ
ビジネスソリューション部
齋藤 壽勝

挑みつづける。求めつづける。

ネットワークの可能性



- 1 . 会社概要
- 2 . 企業での情報セキュリティ対策
- 3 . やらなくてはならない内部統制
- 4 . 内部統制をサポートする Master'sONE
- 5 . Master'sONE
リスクマネージメントサービス

1 会社概要

【設立】 1985年 9月4日

【資本金】 40億円

【株主】 エヌ・ティ・ティピー・シーコミュニケーションズ株式会社

【代表者】 代表取締役社長 石田 守

【売上高】 775億円(2006年3月期実績)

【従業員数】 471名(2006年3月末現在)

【事業内容】

1.ネットワーク事業

2.オンデマンド事業

3.電話サービス事業

4. 上記に関わるネットワーク構築、保守、システム開発等

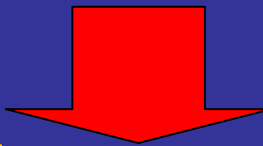
2. 企業での情報セキュリティ対策

2 - 1 情報セキュリティ対策の必要性(1)

企業経営に問われるもの

法令順守(コンプライアンス)
社会的責任(CSR)
情報開示(ディスクロージャー)

企業を取り巻くITに関する
法整備状況



個人情報保護法
日本版SOX法

2 - 2 情報セキュリティ対策の必要性(2)

個人情報保護法(2005年4月施行)

取り扱う個人データの漏えい、滅失、毀損等の防止のための安全管理の処置が必要

日本版SOX法(基準案)が定義する「内部統制」 (2006年法制化 2008年施行)

日本版SOX法では、内部統制の基本的要素に「ITの活用」が盛り込まれ、ITによる内部統制の重要性が強調されている

- ・「組織内の情報」の徹底した管理が不可欠
- ・「情報」が「いつ」「誰に」伝達され、「誰が意思決定をしたか」を随時記録することが重要



日本版SOX法や個人情報保護法により企業の情報システム
・情報セキュリティ体制強化が今まで以上に急務になっている

2 - 3 情報セキュリティ対策とは

内部情報漏洩対策 (日本版SOX法、個人情報保護法)

資産管理 メール・Web閲覧監視・記録(フォレンジック)
メディア持ち出し制限 文書暗号化 ファイルサーバ監視管理

外部からの攻撃対策

不正侵入検知/防御 ファイアウォール

ウィルス・ワーム・クライアント対策

ウィルス対策 スпам対策 アプリケーション利用履歴管理
セキュリティパッチ管理 PC不正接続監視/防止
サーバデータストレージ管理 シンクライアント

2 - 4 情報セキュリティ対策の実態(1)

対処済みのセキュリティ対策

1位	ウイルス対策	91.6%
2位	FW / VPN	68.3%
3位	スパムメール対策	49.9%
4位	ID/アクセス管理	46.2%

・
・
・

IDCジャパン調べ

多くの企業はウイルスソフトのインストールは行っているが、管理までは実施されていないのが現状。実際に管理されているのは30% ~ 40%。

管理とは

ライセンスの更新、セキュリティーパッチ

管理、不正PC接続防止、不正操作防止等

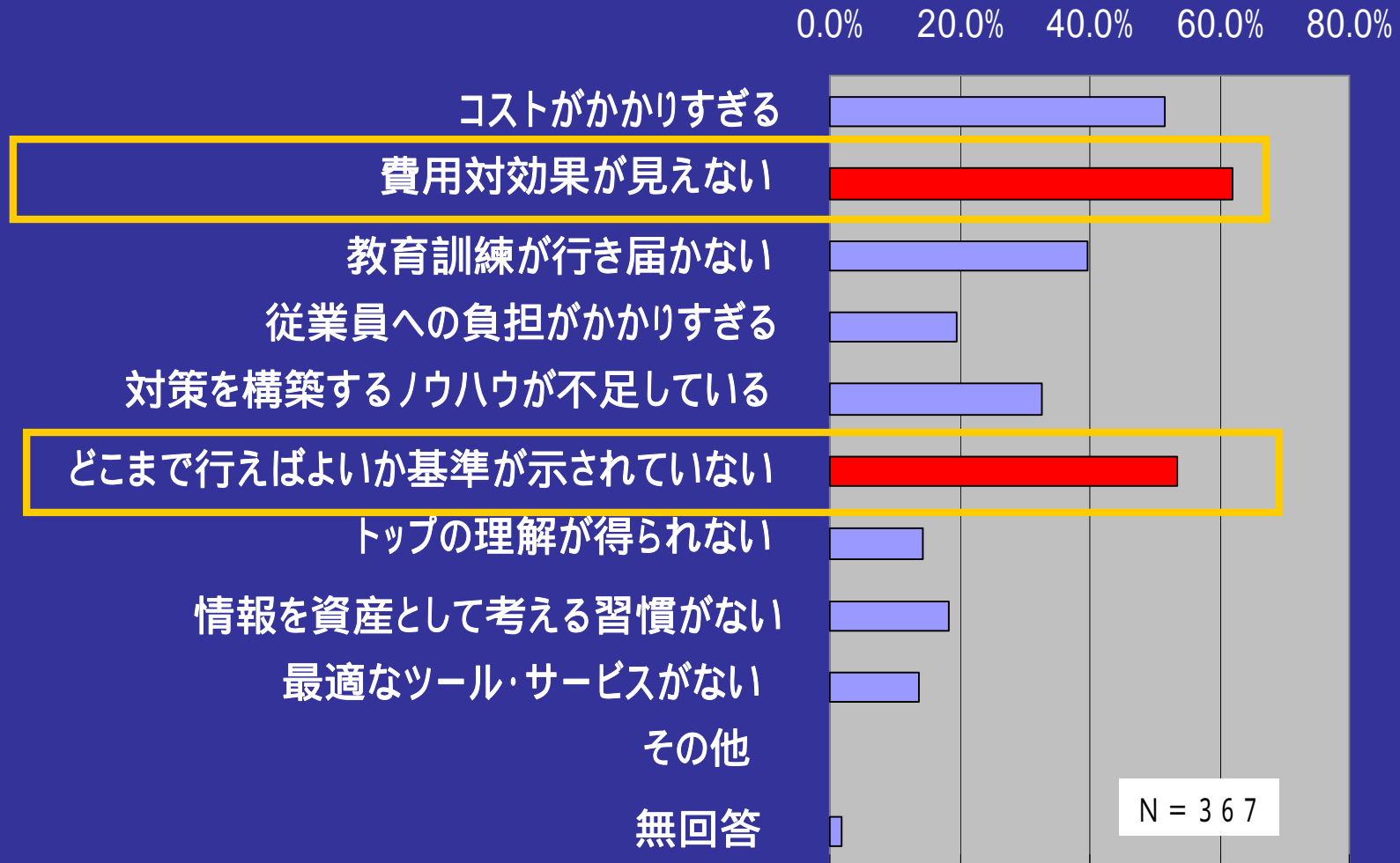
2 - 5 情報セキュリティ対策の実態(2)

導入を検討・予定しているセキュリティ対策

- 1位 不正アクセス監視
 - 2位 セキュリティ教育・トレーニング
 - 3位 ファイアウォール運用管理
 - 4位 セキュリティコンサルティング
 - 5位 セキュリティ検査・監査
- ・
・
・

2 - 6 情報セキュリティ対策の問題

情報セキュリティ対策が行われない理由



2 - 7 対策に積極的になれない要因

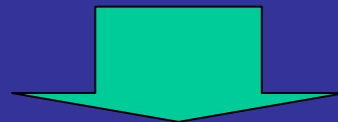
企業が内部情報漏洩対策への取り組みに
積極的になれない要因

セキュリティ事故発生のリスクが明確でない

- ・事故が発生して、初めて重要性を認識させられる
「企業の情報は漏洩しないもの」という思い込みがある為、**事故発生に伴う経済的損失
信用失墜といった企業経営上に対するリスクを冷静に把握することが難しい**

既存の情報セキュリティへの「対策」「取り組み」が
企業価値に直結していない

- ・情報セキュリティの確保は企業活動上では、「裏方」の位置にあることから、その必要性を理解しつつも、対策によるリスク低減や費用対効果がわかりにくいこともあり、**現状情報
セキュリティ対策に積極的に取り組む企業が、ステークホルダーから評価されていない**



適切な情報セキュリティ投資の判断が困難

2 - 8 対策不備による事件

顧客情報流出、不正コピー、アクセス、PC盗難等の 情報漏洩は企業の信頼を失う

大手化粧品会社、顧客情報紛失
不正アクセスによりホームページ
から流出

(2005年1月)

51万人の顧客情報流出。
大手通販会社、事件により減収減益

(2004年3月)

某市役所で情報漏洩発生！
市民1人につき1万円支払いを
命じられる

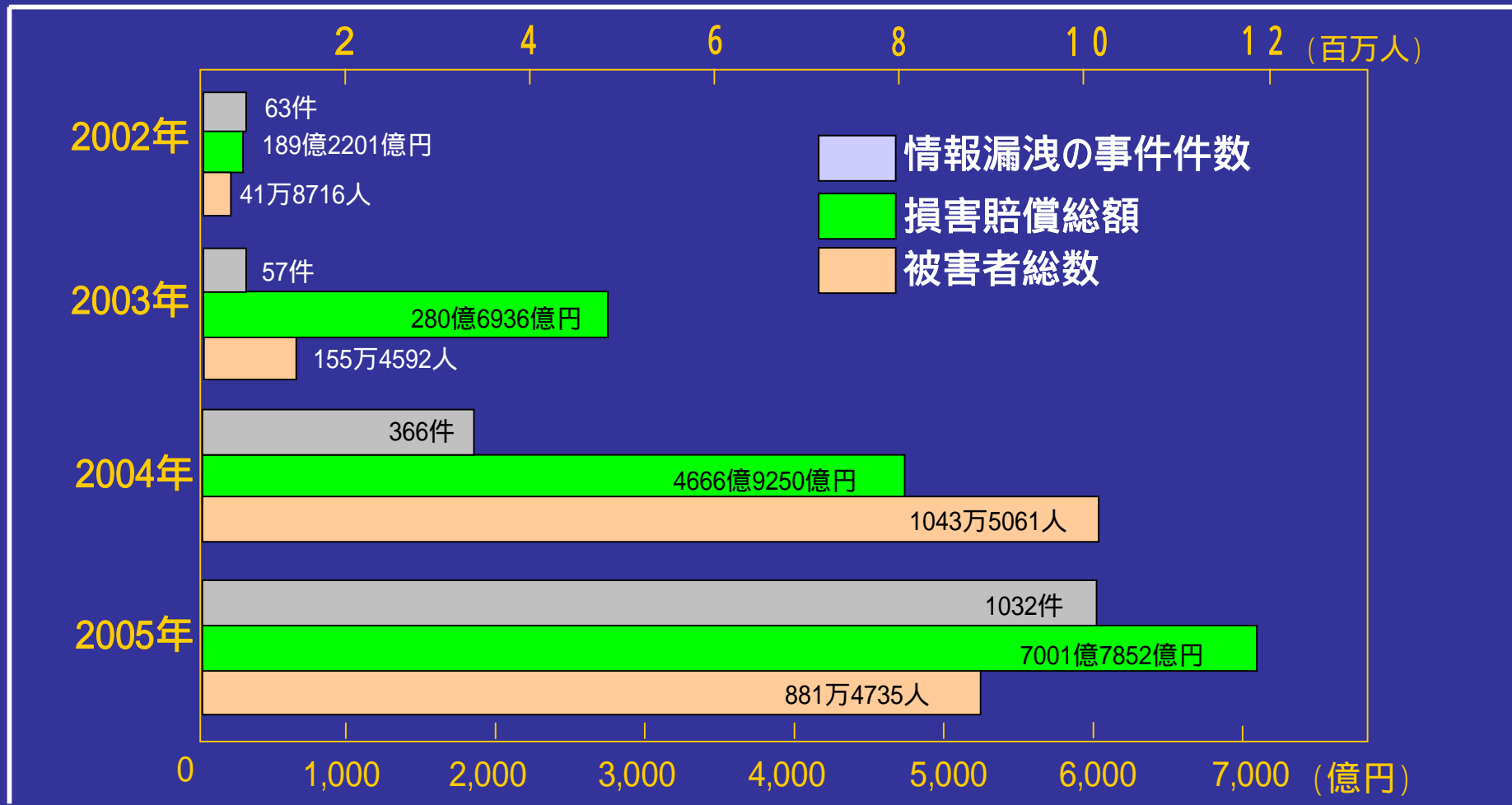
(1999年5月)

中央官公庁、納税者約47万人分の
個人情報記録したPCが所在不明

(2005年9月)

2 - 9 情報漏洩事件の経年変化

情報漏洩事件は毎年増大し、被害者を増やし、
企業における損害賠償が拡大している



自社を守り継続してビジネスを継続・発展

させるためにも

今、企業には統合的なセキュリティ対策が

求められています

特に、内部統制対応が必要となっています

3. やらなくてはならない内部統制

3 - 1 やらなくてはならない内部統制(1)

相次ぐ会計不祥事やコンプライアンス(法令遵守)の欠如などを防止するため、**会計監査制度の充実**と企業の**内部統制強化**を求められた



具体的には、証券取引法の抜本的改正である「**金融商品取引法**」が閣議決定された

- 金融商品取引法 -

金融・資本市場をとりまく環境の変化に対応し、投資者保護のための横断的法制を整備することで、利用者保護ルールの徹底と利用者利便の向上、「貯蓄から投資」に向けての市場機能の確保及び金融・資本市場の国際化への対応を図る



投資家保護が目的

- ・金融商品取引法には、米国のサーベンス・オクスリー法(SOX法)に倣った日本版SOX法(J-SOX法)が盛り込まれている
- ・2008年に**日本版SOX法**が適用される

3 - 2 やらなくてはならない内部統制(2)

従来、財務報告をする際

財務諸表

: 経営者が作成する財務報告書

財務諸表監査報告書

: 公認会計士による財務諸表が適正であることを示す証明書

が必要

日本版SOX法が施行されると上記に加えて、

内部統制報告書

: 財務報告書に係る内部統制の有効性を示す報告書

内部統制監査報告書

: 公認会計士が内部統制報告書が適正であることを示す証明書

が必要



内部統制の整備が義務付けられる

3 - 3 内部統制を整備するには(1)

内部統制とは、どのようなものなのか？

内部統制を考える上での基本的枠組みはCOSOのフレームワークである

日本版COSOフレームワークはCOSOの構成要素に「ITへの対応」が盛り込まれ、IT統制の重要性が強調されている

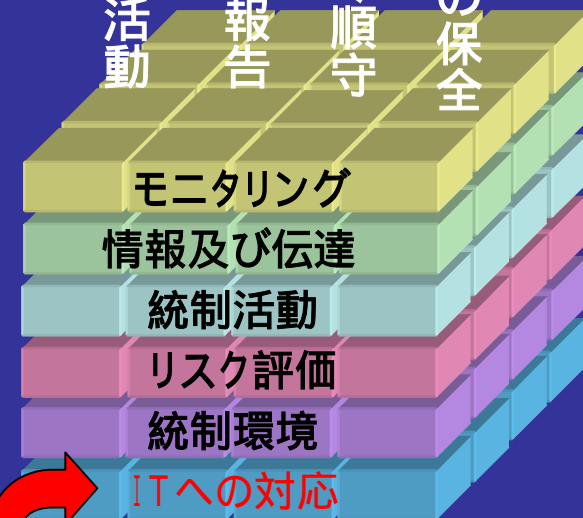
内部統制では
ITの統制・ITを活用した統制が必要

どうすればよいか？ = COBIT

内部統制の目的

業務活動
財務報告
法令順守
資産の保全

内部統制の構成要素



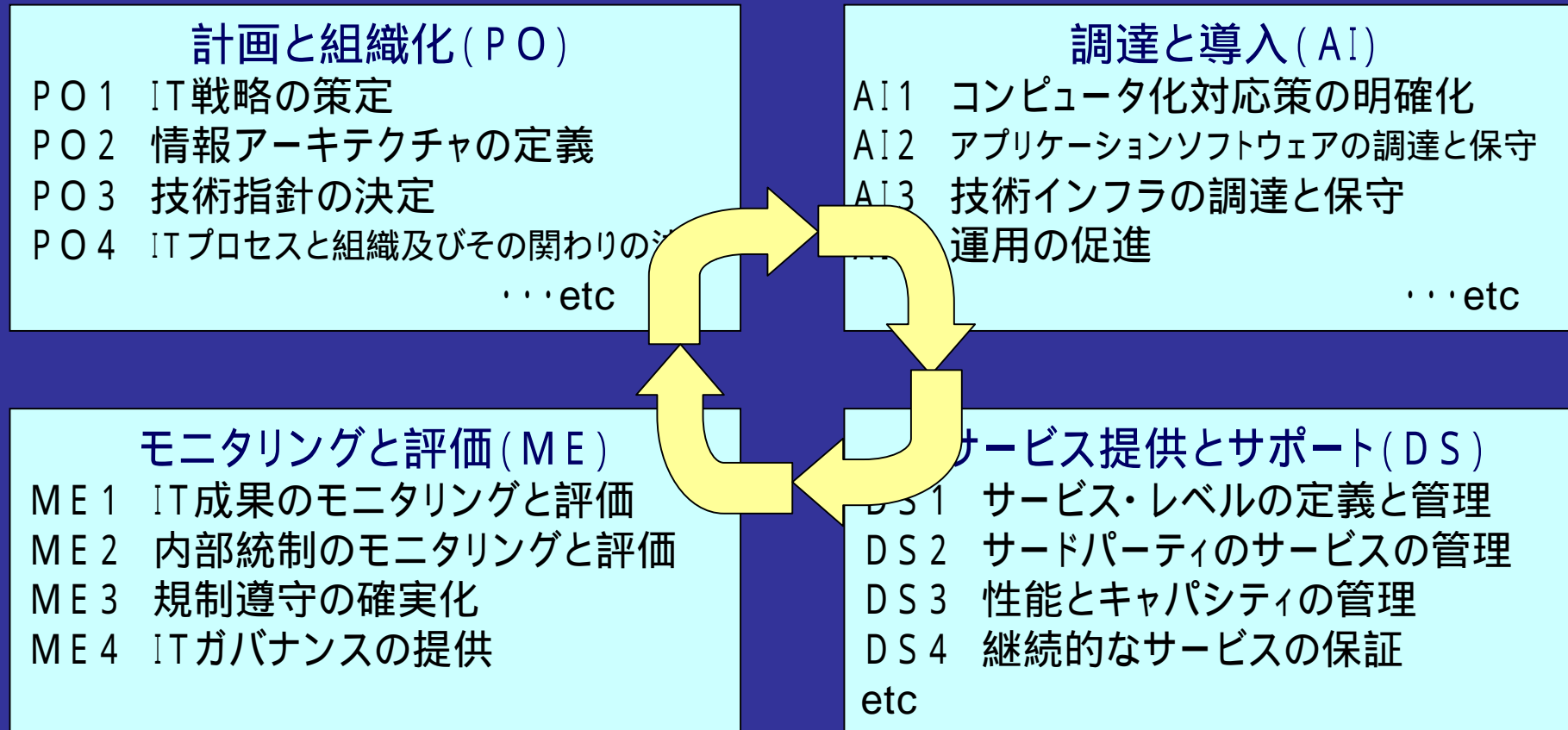
日本版COSOで新しく追加された構成要素

3 - 4 内部統制を整備するには(2)

COBIT (Control Objectives for Information and related Technology)

内部統制のIT管理の基準を示したのがCOBITである

COBITでは、IT活動を4つのドメインと34のプロセスを定義している
さらに、詳細レベルの統制活動で定義している



PO1 IT戦略計画の策定

PO1.1 IT導入価値の把握

PO1.2 事業目的に沿ったITの導入

PO1.3 既存情報システムの現状把握

PO1.4 IT戦略計画の策定

PO1.5 IT実行計画の策定

PO1.6 IT資産の管理



PO9 ITリスクの評価と管理

PO9.1 事業リスク管理に沿ったITリスク管理

PO9.2 リスク要因の明確化

PO9.3 企業内で発生する問題の認知と内容把握

PO9.4 リスク評価

PO9.5 リスク対応

PO9.6 リスク対応計画の管理と監視

DS5 システムセキュリティの保証

DS5.1 ITセキュリティの管理

DS5.2 ITセキュリティ計画

DS5.5 セキュリティテスト、監督、監視

DS5.6 セキュリティインシデントの定義

DS5.9 マルウェアの防止、検知、回収

DS5.10 ネットワークセキュリティ

内部統制を実現するためには

ITの統制・ITを活用した統制が必要で

それを実現するためには

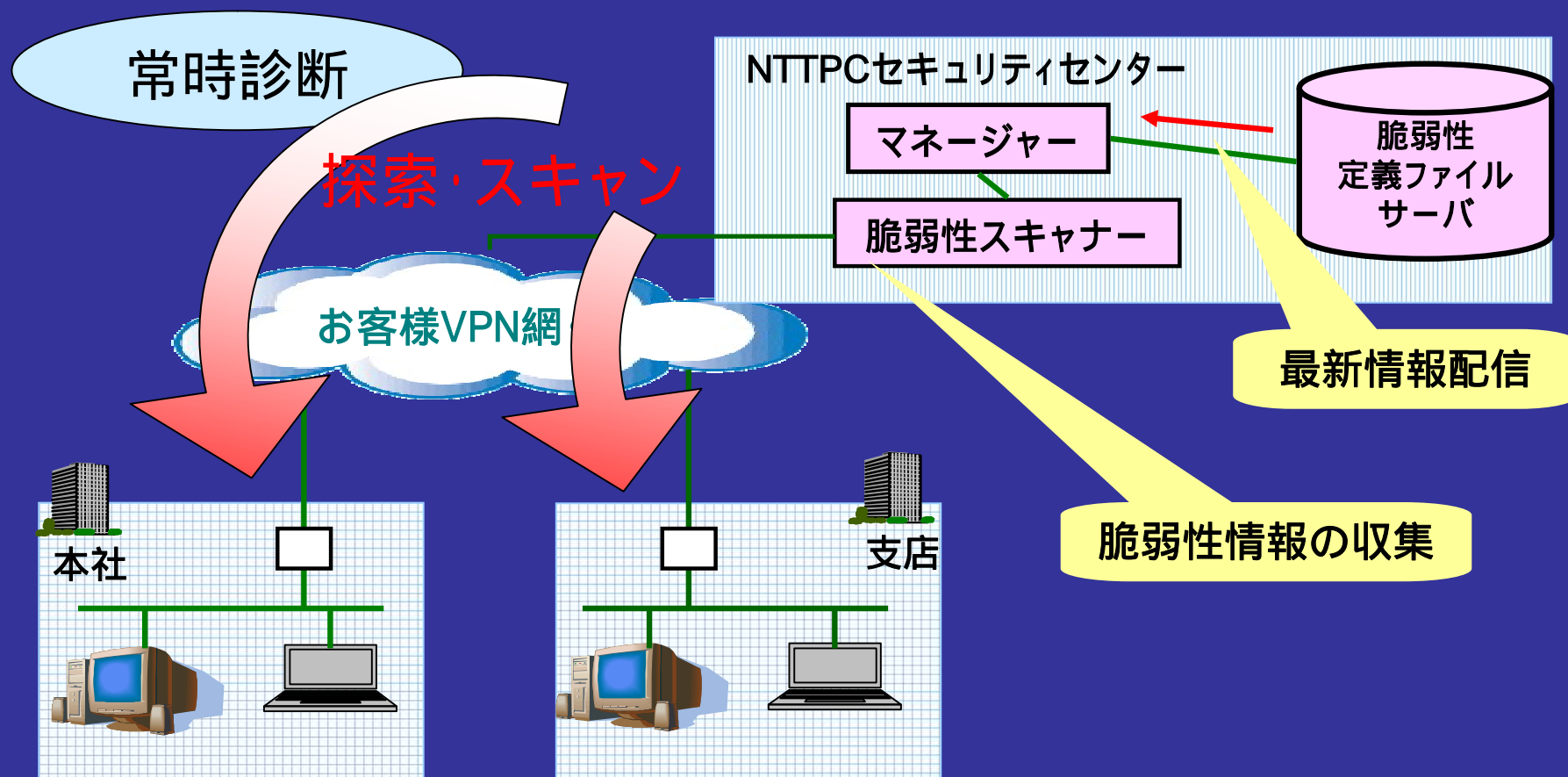
IT統制活動の4つのサイクルを絶えず

行う必要がある

4 . 内部統制をサポートするMaster'sONE

4 - 1 脆弱性診断サービスの概要

Master's ONE 脆弱性診断サービスは 統制活動をサポート！！





4 - 2 脆弱性診断サービスの特長

導入が容易

必要な機器はNTTPC のセキュリティセンター内に設置
エージェントソフトのインストールは不要

クライアントPCの診断

PC 利用者にストレスを与えない負荷の軽い診断方式
約3,000種類のOS、アプリケーションを診断

脆弱性の可視化

独自のスコアリング方式により脆弱性を可視化
セキュリティの専門家でなくても的確な優先順位で対処が可能

PO1 IT戦略計画の策定

PO1.1 IT導入価値の把握

診断によりネットワーク全体のホスト数やどの
のようなOS・アプリケーションがインストール
されているか検出する
これにより管理すべきシステムの状況が把
握できる

PO1.6 IT資産の管理

PO9 ITリスクの評価と管理

検出された脆弱性は、ホスト・アプリケーション
単位でスコアリングされ、脆弱性を可視化する
これにより、対処すべき脆弱性の優先順位づけ
が容易になる

PO9.4 リスク評価

PO9.5 リスク対応

PO9.6 リスク対応計画の管理と監視

DS5 システムセキュリティの保証

インストールされているOSやアプリケーションの脆弱性を検出します
不正アクセス者やウイルスから攻撃を受ける可能性のある端末を特定する

DS5.6 セキュリティインシデントの定義

DS5.9 マルウェアの防止、検知、回収

DS5.10 ネットワークセキュリティ

お客さまサーバ、ネットワーク機器等の脆弱性を診断し、レポートします

システム上のどこに問題があるかを把握し、具体的にどのようなセキュリティ対策を打てばいいのかの指標を得ることができます

レポート例

Master's ONE 脆弱性診断サービス XXXX年 xx月分 診断レポート

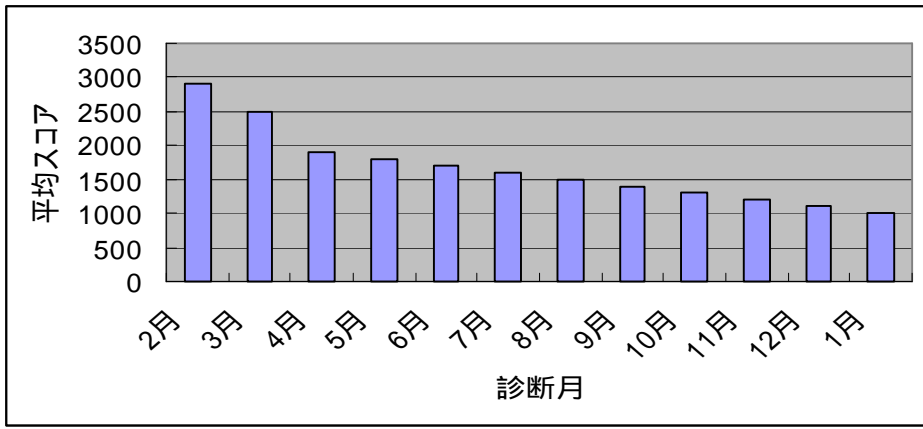
1. サマリーレポート ネットワーク全体の診断結果

検出されたホスト数	100
スコア平均値	1000
診断結果	非常に危険

診断結果とホスト分布

診断結果	ホスト数	ホスト分布
非常に危険	3	33%
危険	0	0%
注意	0	0%
比較的安全	97	67%

平均スコアの推移



レポート例

診断対象ネットワークのホスト一覧をレポートします。IPアドレス
ホスト名 OS 脆弱性のスコア
診断結果 をレポートします

2. 検出されたホストの一覧

IPアドレス	ホスト名	OS	スコア	診断結果
10.233.X.X	SE-XXVER	Windows XP SP2	2402	非常に危険
10.233.X.X	TXXXMOTO	Windows XP (SP0 - SP2)	2376	非常に危険
10.233.X.X	YAXX-DESK	Windows	2376	非常に危険
10.233.X.X	DNS Timed out	FreeBSD 5.2	1	比較的安全
10.233.X.X	DNS Timed out	OS Undetermined	0	比較的安全
10.233.X.X	DNS Timed out	Unix Variant	0	比較的安全
10.233.X.X	DNS Timed out	OS Undetermined	0	比較的安全
10.233.X.X	DNS Timed out	Cisco	0	比較的安全

レポート例

ネットワーク全体の診断だけではなく、ホスト毎に診断結果をレポートします

検出したアプリケーション・検出した脆弱性等、詳しくレポートします

3.ホスト個別レポート

3-1.ホスト 10.233.X.X

ホスト情報

IPアドレス	10.233.X.X	ホスト名	SE-XXVER
OS	Windows XP SP2	診断結果	非常に危険

検出されたアプリケーション

アプリケーション名	ポート/プロトコル
DCE/MS RPC Endpoint Mapper Interface (TCP)	135/TCP
Windows XP Direct SMB Hosting Service	445/TCP
HTTP-Based Application	8181/TCP
McAfee AntiVirus/EPO Agent	8181/TCP
Windows NetBIOS Name Service	137/TCP
Windows XP NBT	139/TCP
Telnet	23/TCP

検出された脆弱性

脆弱性名	危険度
McAfee EPolicy Orchestrator Framework Service Directory Traversal Vulnerability	非常に危険
NetBIOS Name Table	比較的安全
Microsoft Windows Terminal Services Denial Of Service Vulnerability	比較的安全
Telnet Available	比較的安全
DCE RPC mapper available	比較的安全
Windows SMB Packet Signing Disabled	比較的安全



レポート例

検出された脆弱性は、脆弱性の内容・解決策・回避策を脆弱性情報として解説します

4. 各脆弱性の解説

4-1 脆弱性

脆弱性情報

脆弱性名	McAfee EPolicy Orchestrator Framework Service Directory Traversal Vulnerability
カテゴリ	Access Control Breach
危険度	非常に危険
リスクレベル	Remote Privileged
スキルレベル	Windows GUI
CVE	CVE-2006-3623

脆弱性の内容

McAfee ePolicy Orchestrator には、ユーザ入力データを正しくサニタイズしないことによる、リモートのディレクトリトラバーサル脆弱性が存在します。攻撃が成功すると、システムを完全にリスクにさらしてしまう可能性があります。

解決策

ユーザは、McAfee 製品の更新 Web サイトにログインし、ePolicy Orchestrator 3.5.5.438 またはそれ以降のバージョンをダウンロードする必要があります。

また、ePolicy Orchestrator そのものを使用して、この製品の脆弱性がないと報告されているバージョンにアップグレードできます。ベンダからこの脆弱性を修正するパッチがリリースされています。

Microsoft Windows 2000 Service Pack 4

<http://www.microsoft.com/downloads/details.aspx?familyid=3DD3B530-7F43-4C18-8298-6E8797431A5D>

回避策

MicrosoftはPrint Spooler Serviceを無効にすることを推奨していますが、こうするとローカルおよびリモートの印刷も無効となってしまいます。



Master's ONE

脆弱性診断サービスは

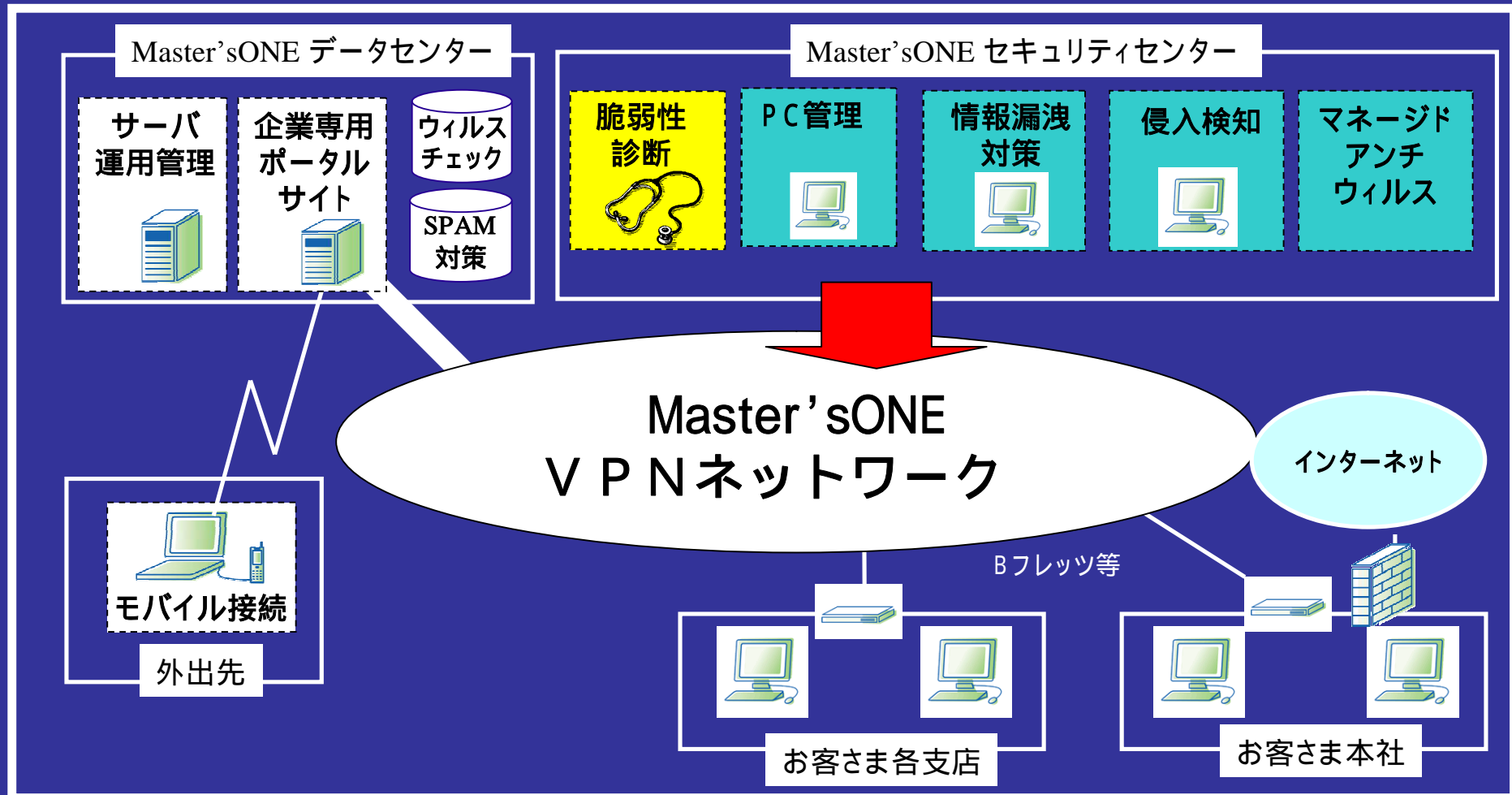
内部統制の整備の強化を

サポートします

5 . Master'sONE

リスクマネージメントサービス

5 - 1 リスクマネジメントサービス



5 - 2 リスクマネージメントサービスの概要(1)

PC管理

資産管理サービス

各拠点のPC端末まで含めた資産の一元管理を実現します
管理されている資産情報と、検出した機器を照合して未管理(不正接続PC)の特定をします

検出した機器は、お客様向け専用ポータルから参照・検索
できます

情報漏洩対策

個人情報漏洩対策サービス(提供予定)

社員のPCを検索し、個人情報(住所、電話番号、メールアドレス)等が記述されているファイルを特定し、重点管理を促すサービスです

5 - 3 リスクマネージメントサービスの概要(2)

侵入検知

ゲートウェイ・セキュリティ運用監視サービス

ファイアーウォール、侵入監視/リアクション、アンチ・ウィルス(スパイウェア対策含む)、アンチ・スパム(フィッシング対策含む)、URLフィルタという、ゲートウェイ・セキュリティとして必要と考えられている全ての機能の運用と監視を行うサービスです

マネージドアンチウィルス

マネージドアンチウィルスサービス(提供予定)

パターンファイルの更新状況管理など、アンチウィルスソフトの運用を代行し、システム管理者様の負荷を軽減するサービスです

Master's ONEは

企業の信頼性を守る

セキュリティサービスの新たな形態を

ご提案します

THANK YOU !

お問い合わせ
(株)NTTPCコミュニケーションズ

ビジネスソリューション部
E-mail:msone@nttpc.co.jp
TEL:03 - 5212 - 1380

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