

日本版SOX法と これからのセキュリティ対策

2007年2月7日

(株)NTTPCコミュニケーションズ
オンデマンド事業部

1. 2006年度を振り返って
2. 日本版SOX法の中の内部統制
3. 日本版SOX法の中のIT
4. 日本版SOX法とセキュリティ
5. NTTPCのアプローチ
6. SecurityBOSS
7. SecurityBOSSのサービス群
8. まとめ

1. 2006年度を振り返って

1-1. 2006年度の主なセキュリティ動向

IT関連事件

終わらない情報漏えい

- ・ Winny関連事件続出(総務省16億円の対策費用要求)
- ・ Winny開発者の金子氏1審で有罪判決(上告)

0円の影響

- ・ SOFTBANK Mobile MNPの受付過多でシステム障害

MP3プレーヤーもウイルス感染

- ・ マクドナルドのキャンペーン賞品のMP3プレーヤーがウイルスに感染していることが分かり、1万台を回収
- 何でも攻撃対象になってしまう時代へ

社会の動き

セキュリティ意識の高まり?

- ・ 政府が2月2日を「情報セキュリティの日」と制定

コンプライアンス

- ・ 新会社法施行
 - ・ 金融商品取引法成立(2008年度より施行): いわゆるJ-SOX法
内部統制報告書の内容、評価、監査方法は別途内閣府令で定める
- 明確にITも含んだ内部統制の要請

2. 日本版SOX法の中の内部統制

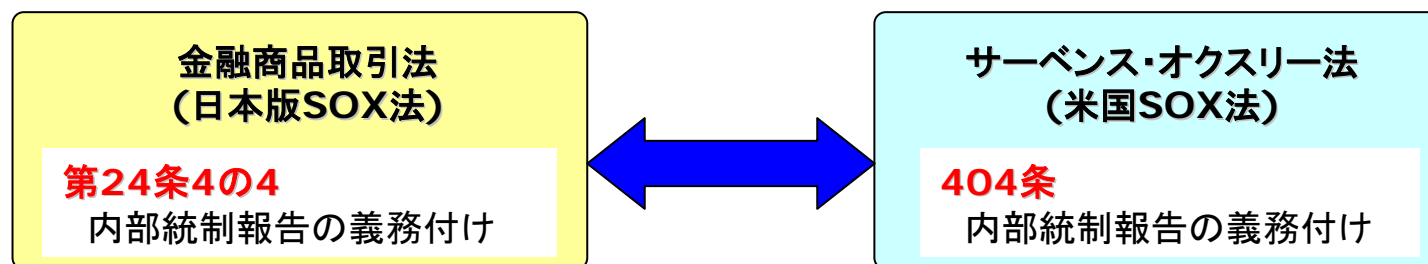
2-1. 金融商品取引法 (旧 証券取引法)

概要

- 元々証券取引法であったが、2006年の改正の際、金融先物取引法などの投資商品に関する法律群をこの法律に統合し、名称が「金融商品取引法」に改題されることとなった

第24条4の4

- 事業年度ごとに、公認会計士等によって監査された、財務報告に係る内部統制報告書を内閣総理大臣に提出することを義務付ける
- 内部統制の内容、実施基準、評価基準については内閣府令により別途定めることが記載されているが、金融庁 企業会計審議会 内部統制部会の作業部会が作成した、「財務報告に係る内部統制の評価及び監査に関する実施基準」(現在2006/11/21版の公開草案)が元となる見通し



金融商品取引法が日本版SOX法と
言われる所以

2-2. 新会社法の中の内部統制との違い

日本版SOX法の内部統制		新会社法の内部統制
株式公開会社(上場企業約3,800社)とその連結子会社	対象企業	大会社(資本金5億円以上または負債200億円以上の会社)
有価証券報告書(財務報告)への記載事項の信頼性の確保を求めている	目的	事業活動全般の業務の適正化を求めている
経営トップが内部統制の有効性を評価し、それを会計士が監査することを求めている	評価方法	内部統制を実現するための仕組みの方針の決定を義務付けている。監査に関する規定はない
金融庁 企業会計審議会内部統制部会の作業部会が「実施基準」を作成予定	指針	法務省の「会社法施行規則」で定める
虚偽記載など最も重い場合、10年以下の懲役または1,000万円以下の罰金(金融商品取引法)	罰則規定	なし(内部統制の仕組みを作っていないなどと認められた場合、株主代表訴訟の対象となる可能性がある)

参考: 日経コンピュータ 特別編集版「待ったなし 内部統制」

2-3. 実施基準の概要

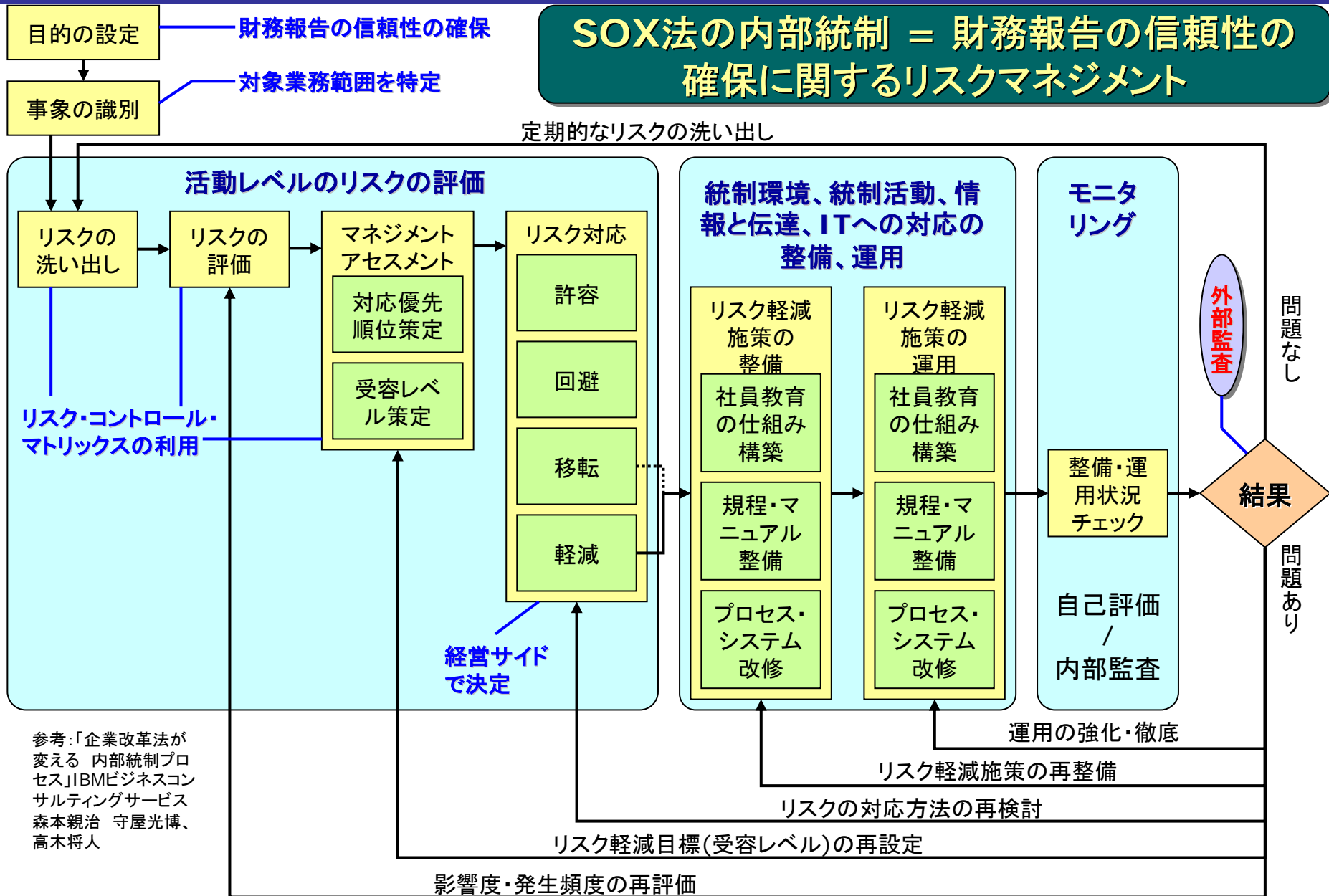
財務報告に係る内部統制の評価及び監査に関する実施基準 公開草案

- 金融商品取引法で義務付けられた内部統制報告書の内容、評価、監査の実施基準になるとされる文書(11/21)。他国と比べ、ITへの対応が特徴的。
- これを受けて経済産業省が「システム管理基準 追補版(財務報告に係るIT統制ガイダンス)」草案を公開(1/19)。COBIT for SOXを意識。

	日本版	米国版
目的	業務の有効性及び効率性	Operations
	財務報告の信頼性	Financial Reporting
	事業活動に関わる法令等の遵守	Compliance
	資産の保全	-
要素	統制環境	Control Environment
	リスクの評価と対応	Risk Assessment
	統制活動	Control Activities
	情報と伝達	Information & Communication
	モニタリング	Monitoring
	ITへの対応	-
ベース	原則主義(経営者の裁量の余地を残す)	規則主義(経営者の裁量の余地がない)
対象範囲	経営者が判断(全業務の60-70%程度)	法で規定(全業務の90%程度)
評価方法	不備、重大な欠陥の2種類	不備、重大な不備、重大な欠陥の3種類
監査方法	インダイレクト・レポーティング	ダイレクト、インダイレクト・レポーティング

COBIT = Control Objectives for Information and related Technology、米国のIT内部統制の指針

2-4. 対応するための一般的な手順 (PDCAサイクル)

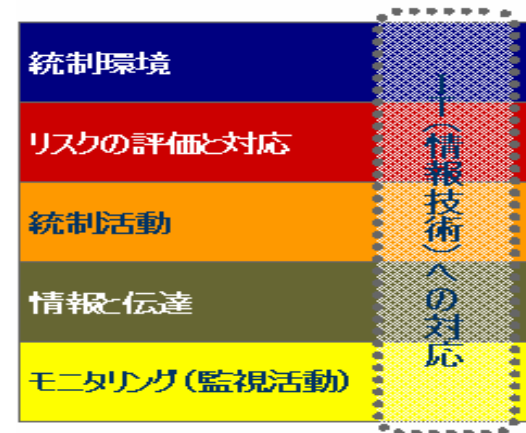


3. 日本版SOX法の中のIT

3-1. 「ITへの対応」と他の統制要素との関係

「ITへの対応」の位置付け

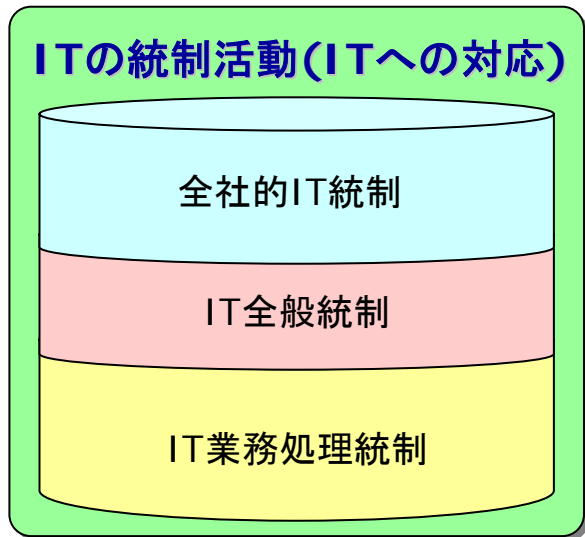
- ITは実態として全社の環境の一部として存在することから、他の統制要素各々の一部として機能することが想定される。



出展：経済産業省「システム管理基準 追補版(財務報告に係るIT 統制ガイダンス)」草案

統制要素	統制要素の有効性を確保するためのITの利用
統制環境	統制環境の整備及び運用を効率的に行う手段 (例) Emailの利用で経営の意思決定を適切な人間に適時に伝達する
リスクの評価と対応	リスクの評価と対応をより有効かつ効率的に機能させる手段(事象の認識、情報共有) (例) 債権管理の自動化により、回収漏れのリスクを低減する
統制活動	業務プロセスの統制活動の自動化の手段 (例) 棚卸し機能付き生産管理システムの開発により、適時に帳簿上の在庫と実在庫の差を把握できるようにする
情報と伝達	組織内部での情報伝達的手段を効果的に業務プロセスに組み込む手段 (例) 必要な承認や作業完了が一定期間に実施されないと、その旨が担当者の上司に伝達される機能を、業務プロセスに組み込む
モニタリング	網羅的なモニタリングを自動的に実施する手段 (例) 日々の業務活動に日常的なモニタリング(ロギング)機能を実装することで、独立的評価のコストを下げる(頻度の低減、投入人員の削減など)

3-2. SOX法の中のIT統制の成り立ち



各統制の役割

IT全社的統制

全般統制と業務処理統制の基礎となる方針、手続きなど。経営者が決定する(全社、事業部、事業所単位)。

IT全般統制

アプリケーション・システムが適切に稼動する環境を保障するIT基盤の統制(IT基盤単位)。

IT業務処理統制

アプリケーション・システム・レベルの統制。個々の財務データとその処理の直接的な統制(アプリケーション・システム単位)。

→ これらが有機的に結び付いて財務報告の信頼性を確保する。

統制の目標	有効性及び効率性	情報が業務に対して効果的、効率的に提供されていること
	準拠性	情報が関連する法令や会計基準、社内規則等に合致して処理されていること
	信頼性	情報が組織の意思・意図に沿って承認され、漏れなく正確に記録・処理されること(正当性、完全性、正確性)
	可用性	情報が必要とされるときに利用可能であること
	機密性	情報が正当な権限を有する者以外に利用されないように保護されていること

統制の目的

財務報告の信頼性確保 = 会計上の取引記録の正当性、完全性及び正確性の確保

各統制の内容

- ・ ITに係る戦略、方針、計画、手続きなどの決定
- ・ ITの開発、保守に係る管理
- ・ システムの運用・管理
- ・ 内外からのアクセス管理などシステムの安全性の確保
- ・ 外部委託に関する契約の管理
- ・ 入力情報の完全性、正確性、正当性等を確保する統制
- ・ 例外処理(エラー)の修正と再処理
- ・ マスタ・データの維持管理
- ・ システムの利用に関する認証、操作範囲の限定などアクセスの管理

4. 日本版SOX法とセキュリティ

4-1. SOX法のIT統制とセキュリティとの関係

SOX法のIT統制			セキュリティ
統制の種類	統制の内容	具体策	考慮すべきセキュリティ要素
全社的IT統制	戦略、方針、計画、手続きなどの決定	統制ポリシーの策定と運用	セキュリティ・ポリシーの策定と運用
IT全般統制	ITの開発、保守に係る管理	システム開発、保守手順の作成と運用	改ざん防止、不正開発防止策の実施など
	システムの運用・管理	システム運用、管理手順の作成と運用	入退室管理、障害対策
	外部からのアクセス管理などシステムの安全性の確保	各種セキュリティ対策の実施	NWセキュリティ、IT基盤の可用性の確保、IT基盤へのアクセス制御/認証の強化、モニタリング、社内LAN全体の健全性の確保
	外部委託に関する契約の管理	契約先の統制状況の確認	契約先のセキュリティ対策状況の確認
IT業務処理統制	入力の完全性、正確性、正当性の確保	入力エラーチェックなど	—
	例外処理の修正と再処理	例外処理の実装	システム(ソフトウェア)の安定性の確保
	マスタ・データの維持管理	データベースの可用性の確保	ストレージの可用性の確保、データ改ざん防止策、認証強化
	システムの利用に関するアクセス管理	アクセス制御	アクセス制御、認証の強化

4-2. 通常のセキュリティ対策との違い

通常のセキュリティ対策 (ISMSなど)		SOX法のセキュリティ対策
全社、事業部、事業所という組織単位	対象範囲	財務報告に多大な影響を与える可能性がある と経営者が判断した業務
機密性、完全性、可用性という視点で分類	情報資産の分類	機密性、完全性、可用性で分類した情報を、 財務報告に与える影響が大きい情報かどうかと いう視点で再分類
機密性、完全性、可用性をそれぞれ高める(機 密性を重視する)	統制施策の方向 性	会計上の取引記録の正当性、完全性及び正 確性を確保する(完全性を重視する)

SOX法のセキュリティ対策

範囲

通常のセキュリティ対策の一部

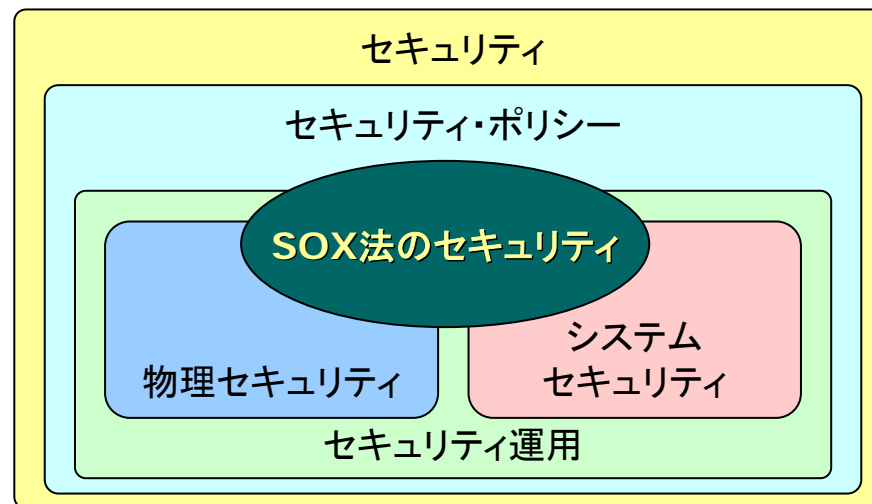
分類

財務報告に影響が高いかどうかと
いう視点

→ 通常のセキュリティ対策の分類の
後、さらにもう一つ軸を設けて分
類する

統制施策

財務報告の信頼性を確保できるか
どうかという観点から施策を策定



範囲は限定されるものの、セキュリ
ティの全ての要素に関する対応が
必要となる

5. NTTPCのアプローチ

5-1. SOX法対応で成功するために – 対応コストの削減

とにかくお金が掛かる

- ・ IDC Japanは、2009年には7,000億円がITにおけるSOX法対応費用になると予測している。

外部コンサル費用

ノウハウの外注費用

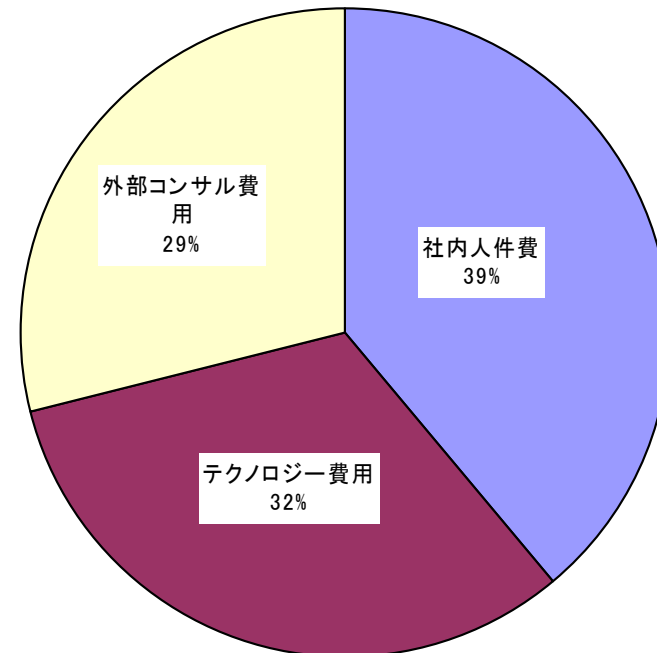
テクノロジー費用

セキュリティ・ポリシーに基づくIT投資

社内人件費

リスクの洗い出し、プロセスの文書化など
最も高くつく部分

2006年のSOX法対応コスト(米国)



出展: AMR SOX法対応コスト調査

支出を極小化するために(一般論)

コンサル費用の削減

必要最小限の範囲を見極めて、自社に必要な対策だけを打つ

テクノロジー費用の削減

アウトソーシングも視野に入れ、効率的な実装を心がける

社内人件費の削減

上記の削減策の相乗効果で劇的に下げることが可能

5-2. SOX法のセキュリティ対応要素の分析

SOX法のIT統制			セキュリティ
統制の種類	統制の内容	具体策	考慮すべきセキュリティ要素
全社的IT統制	戦略、方針、計画、手続きなどの決定	統制ポリシーの策定と運用	セキュリティ・ポリシーの策定と運用
IT全般統制	ITの開発、保守に係る管理	システム開発、保守手順の作成と運用	改ざん防止、不正開発防止策の実施など
	システムの運用・管理	システム運用、管理手順の作成と運用	入退室管理、障害対策
	外部からのアクセス管理などシステムの安全性の確保	各種セキュリティ対策の実施	NWセキュリティ、IT基盤の可用性の確保、IT基盤へのアクセス制御/認証の強化、モニタリング、社内LAN全体の健全性の確保
	外部委託に関する契約の管理	契約先の統制状況の確認	契約先のセキュリティ対策状況の確認
IT業務処理統制	入力の完全性、正確性、正当性の確保	入力エラーチェックなど	—
	例外処理の修正と再処理	例外処理の実装	システム(ソフトウェア)の安定性の確保
	マスタ・データの維持管理	データベースの可用性の確保	ストレージの可用性の確保、データ改ざん防止策、認証強化
	システムの利用に関するアクセス管理	アクセス制御	アクセス制御、認証の強化

ISO9001、14001、ISMS
取得のノウハウを生かした
業務分析とコンサル

ポリシー策定
手順化、文書化

数多くの経験を元に、
お客様の要望に見合った
システム開発や再構築

システムの個別開発、改変
(個別的アプローチ)

汎用性と柔軟性を兼ね備えた
伝統あるNTTPCサービスを、
セキュリティの観点からさらに
強化、充実！

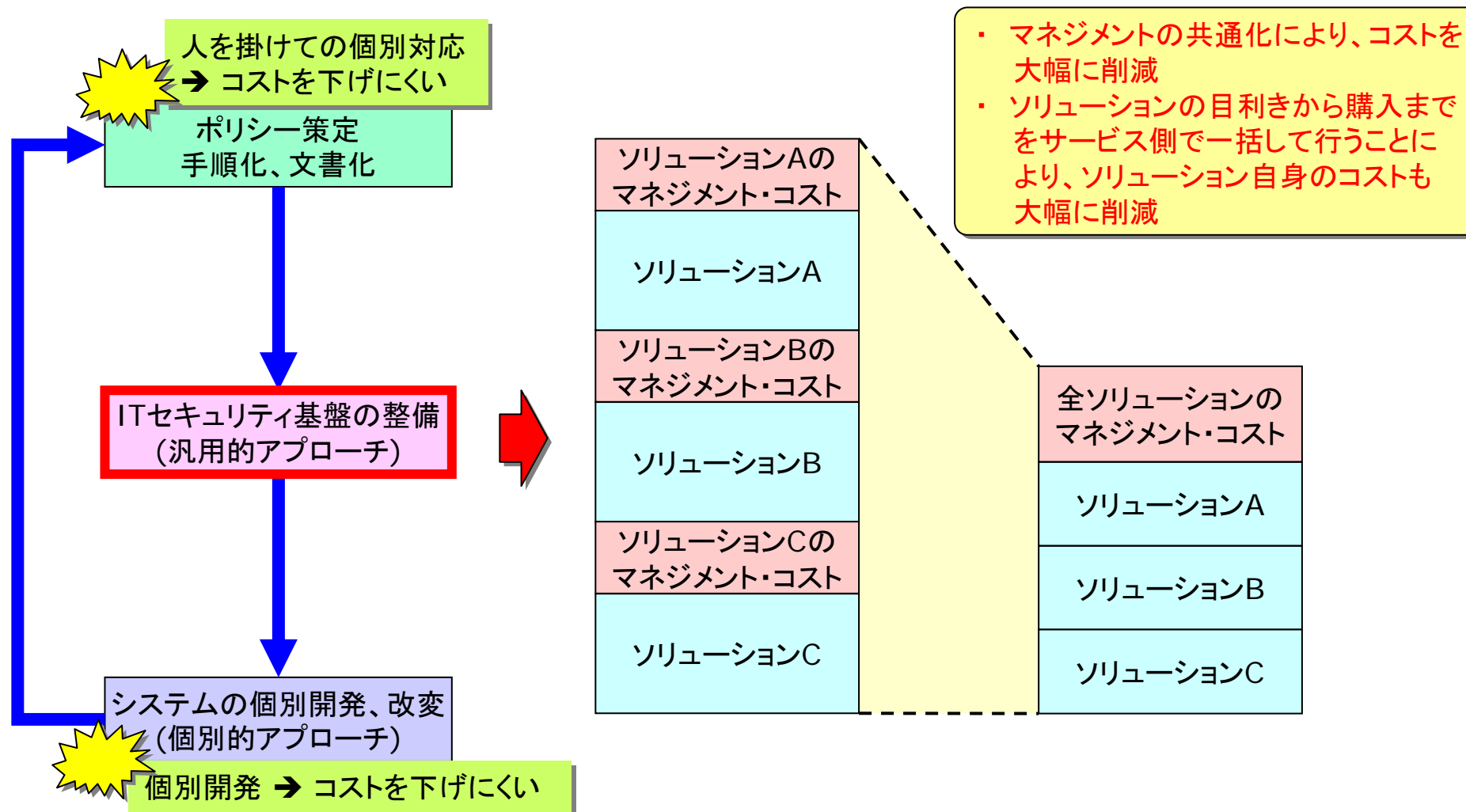
ITセキュリティ基盤の整備
(汎用的アプローチ)

ここに注目！

5-3. 費用削減のポイント

下げ易いところを徹底して下げる

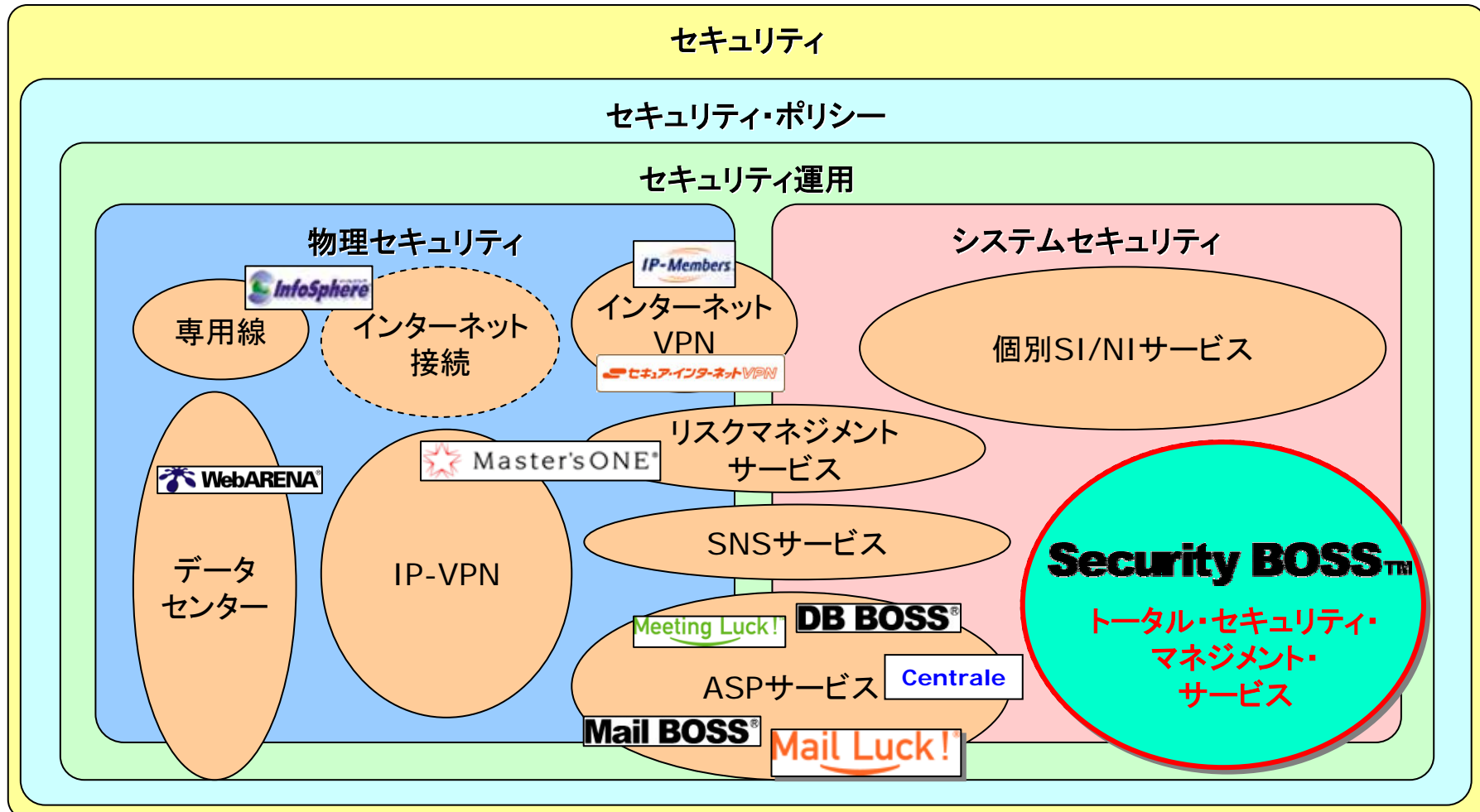
- 各企業の業務にあわせた個別対応が必要な部分や、どうしても人を掛けてやらなければならない部分のコストは下げにくいので、IT基盤を下げる



5-4. NTTPCの商材とセキュリティ

ITセキュリティ基盤のコストを下げるために

ITセキュリティ基盤の部分をカバーするために、既存のサービスでは足りなかった部分を、**トータル・セキュリティ・マネジメント・サービス Security BOSS**として新たにラインナップに加える



5-5. NTTPCの提案

ITセキュリティ基盤の整備 (汎用的アプローチ)

- ・ 専用線、VPN、インターネット接続、データセンター、各種セキュリティ・サービスをISMS準拠レベルで運用し、ITセキュリティ基盤のトータルアウトソーを実現
- ・ お客様に合わせた柔軟な対応が可能
- ・ サービスではどうしてもフィットしない場合でも、全国規模のネットワークを構築してきたノウハウを生かして、個別インテグレーション、運用体制で対応可能

個別の製品やツールをその都度導入する、従来の割高な手法から脱却し、トータルなセキュリティ・サービスを利用して、全体のコストを下げるという発想

トータル・セキュリティ・マネジメント・サービス SecurityBOSS

ポリシー策定 手順化、文書化

- ・ ISMS取得企業であるNTTPCのサービスは、コンプライアンス上、アウトソース先として必要十分
- ・ 利用できるサービスを意識した手順化、文書化を実施することで、アウトソース部分の文書化作業の極小化

システムの個別開発、改変 (個別的アプローチ)

- ・ 各種サービスの利用で個別開発の範囲を最小限に留め、残りの部分を効率よく開発
- ・ お客様の要望をサービス・サイドにフィードバックし、サービス化を検討

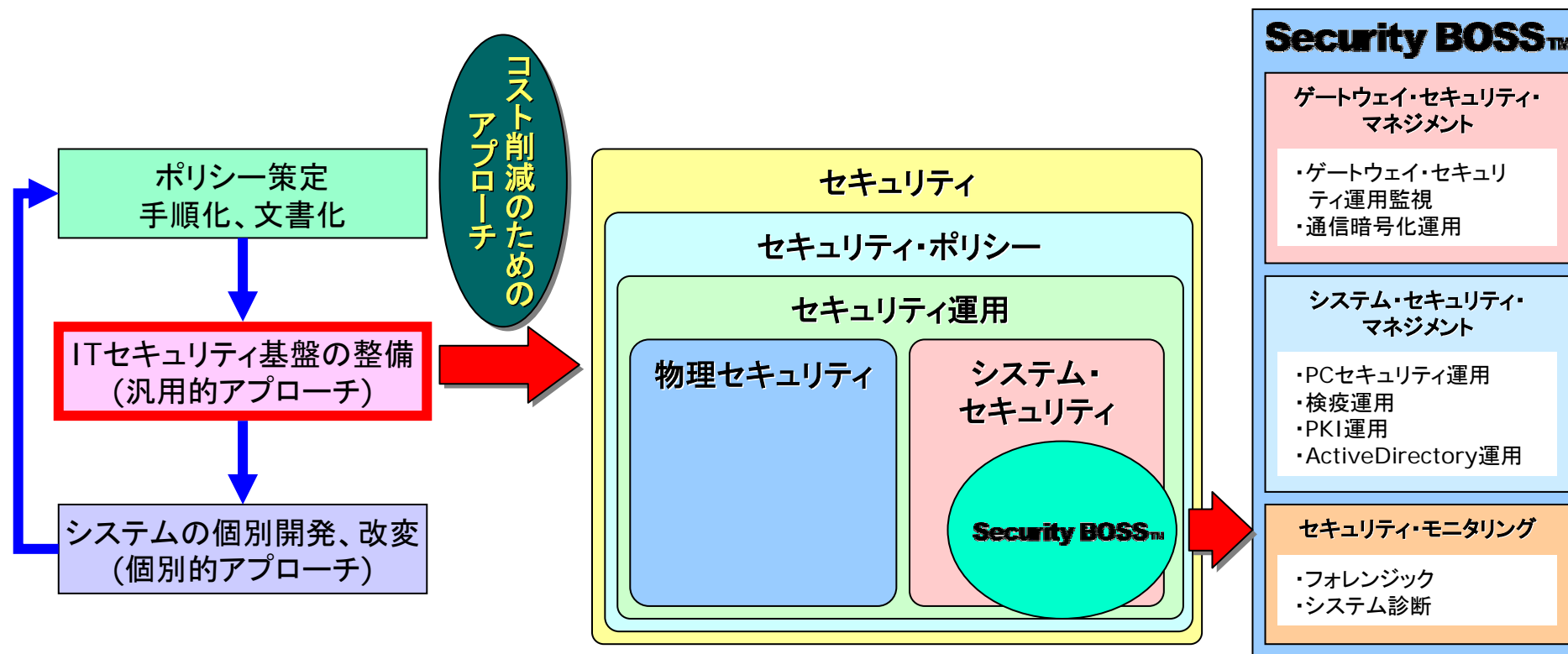
6. *SecurityBOSS*

6-1. SecurityBOSSの目的

SecurityBOSSとは

システム・セキュリティのマネジメントをトータルに提供することで、ITセキュリティ基盤のトータル・アウトソースを可能にし、コンプライアンス対応コストを劇的に削減するサービス群。3つのカテゴリー8つのサービスで、システム・セキュリティをトータルにカバーするトータル・セキュリティ・マネジメント・サービスです

BOSS = BSS & OSS (Business Support Services & Operation Support Services)



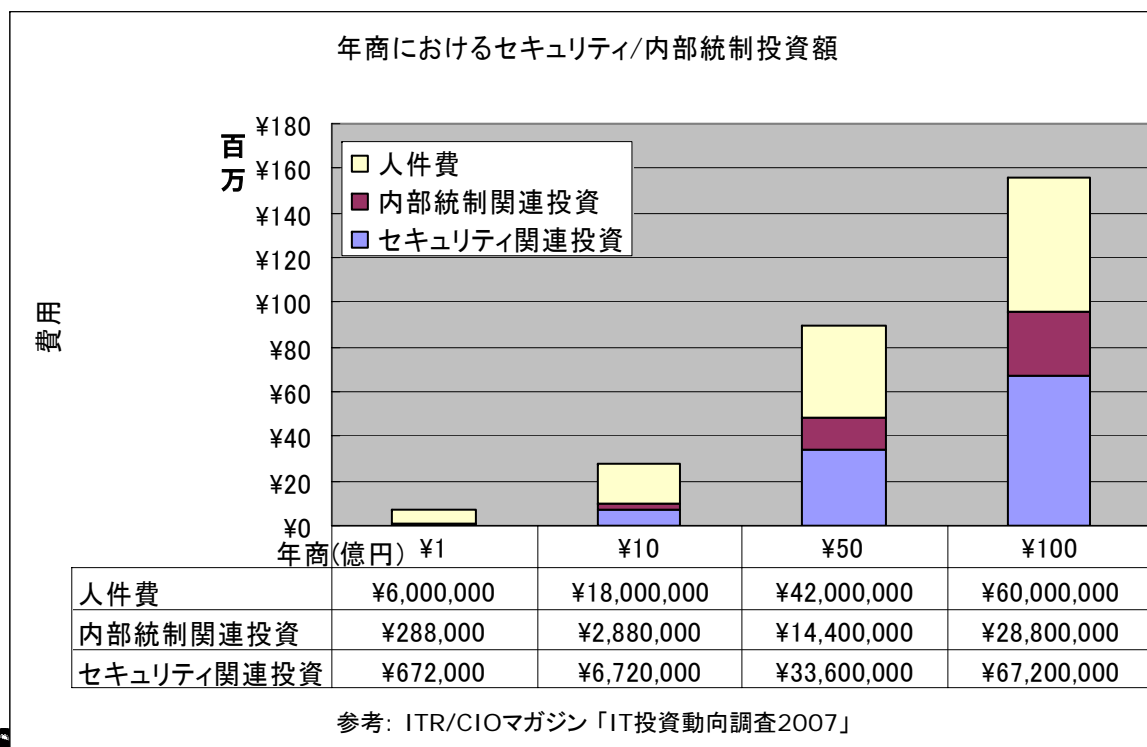
6-2. Security BOSSの特徴 – マネジメント・サービス

最も高価なのは人

ITRとCIOマガジンの調査によれば、2007年はIT関連投資が平均で年商の3.2%となり、過去最高となることが分かった

しかしその一方で、最も高価なのは依然として投資したシステムを運用する人間である

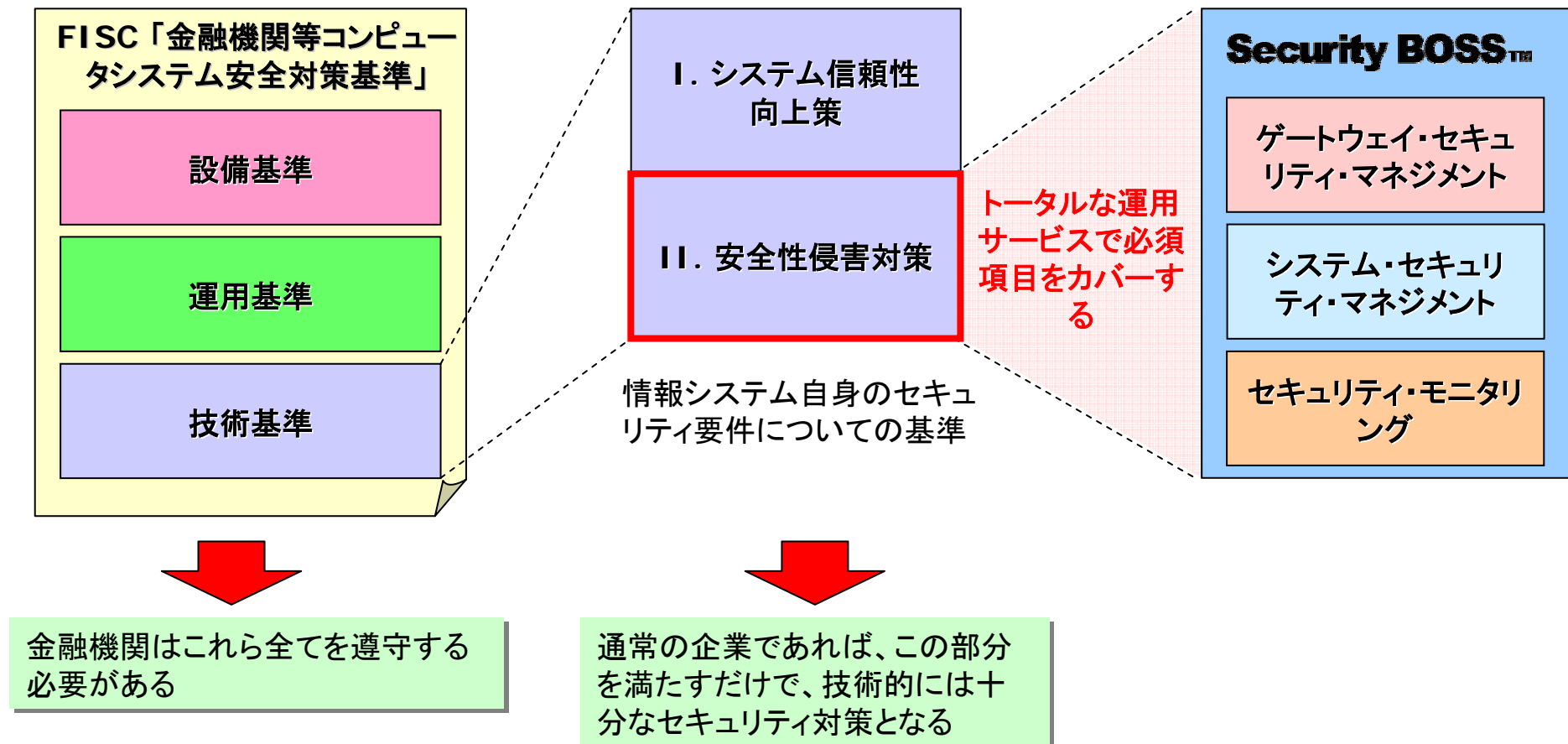
Security BOSSはセキュリティのマネジメントを安心して任せられるサービスを目指し、ISMSに準拠した運用方法で各サービスを提供します



6-3. Security BOSSの特徴 – トータル・サービス

必要十分な提供範囲を用意

金融機関が準拠する、金融庁の外郭団体であるFISC(金融情報システムセンター)のガイドラインのうち、情報システムに関する基準の必須項目の部分を全てカバーすることで、必要十分な範囲のサービスを提供します

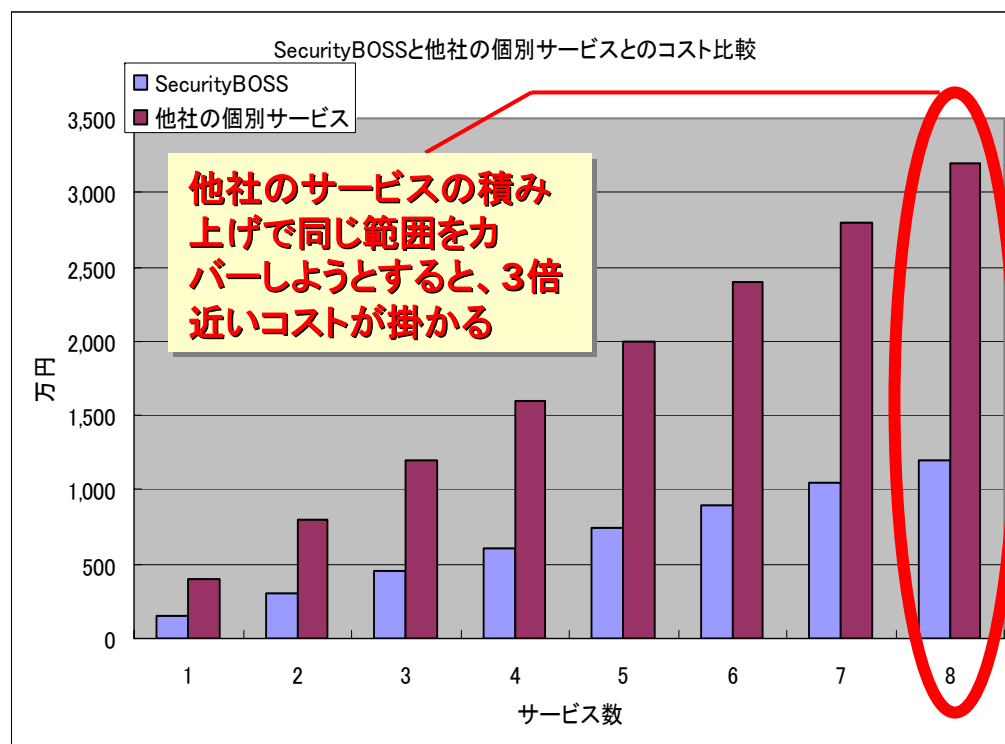


6-4. Security BOSSの特徴 – 低価格サービス

抜群のコスト・パフォーマンス

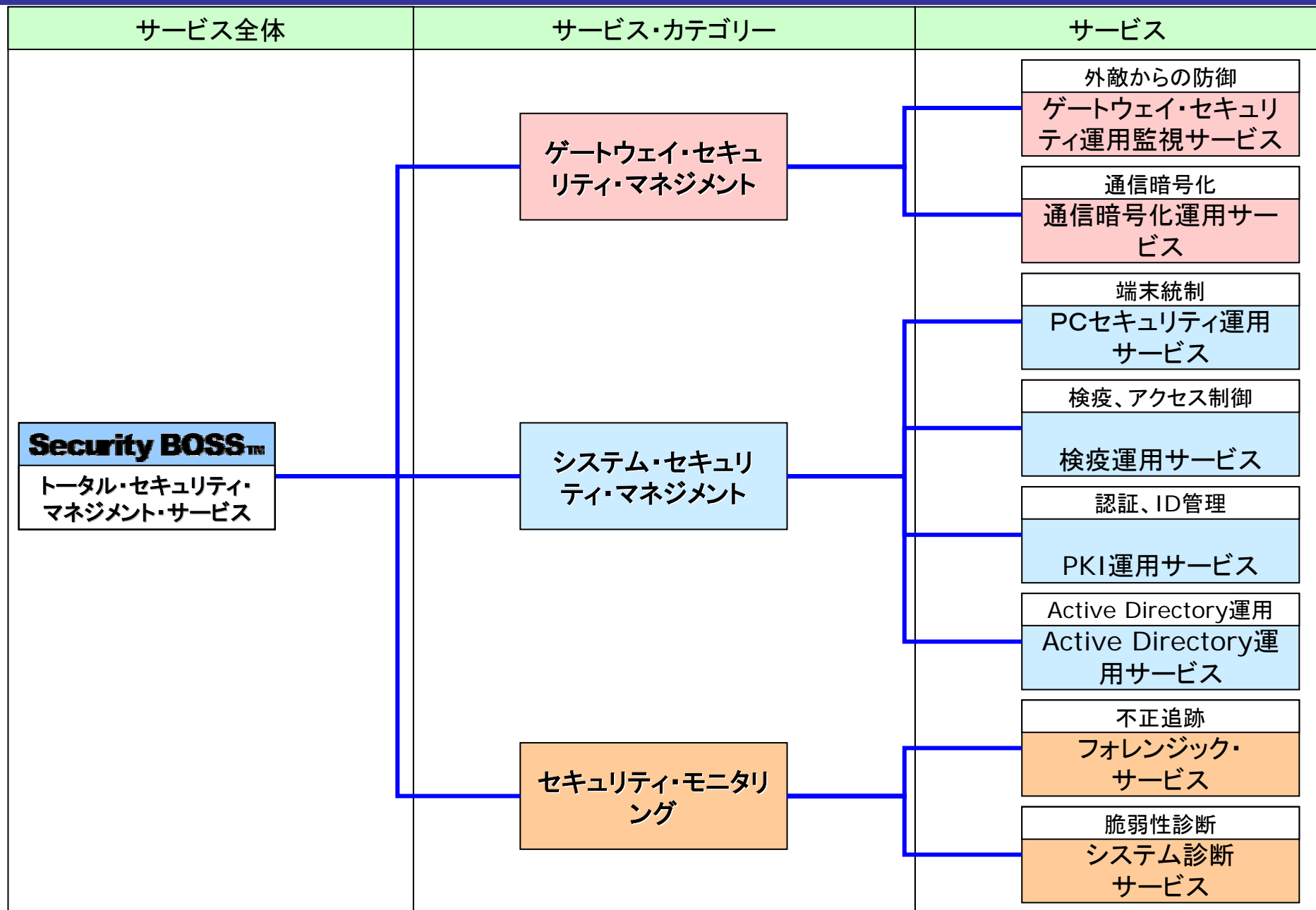
他社のセキュリティ関連サービスが、1つのサービスで情報システム技術者0.5～1人の価格であるのに対し、Security BOSSは8つのサービスで1人程度の価格設定となっており、カバー範囲に対して抜群のコスト・パフォーマンスを発揮します

	SecurityBOSS	他社サービス
1サービス/年(平均値)	150万円	400万円
全てをカバーする費用/年(8サービス)	1,200万円	3,200万円



7. *SecurityBOSS*のサービス群

7-1. SecurityBOSSのサービス・マップ

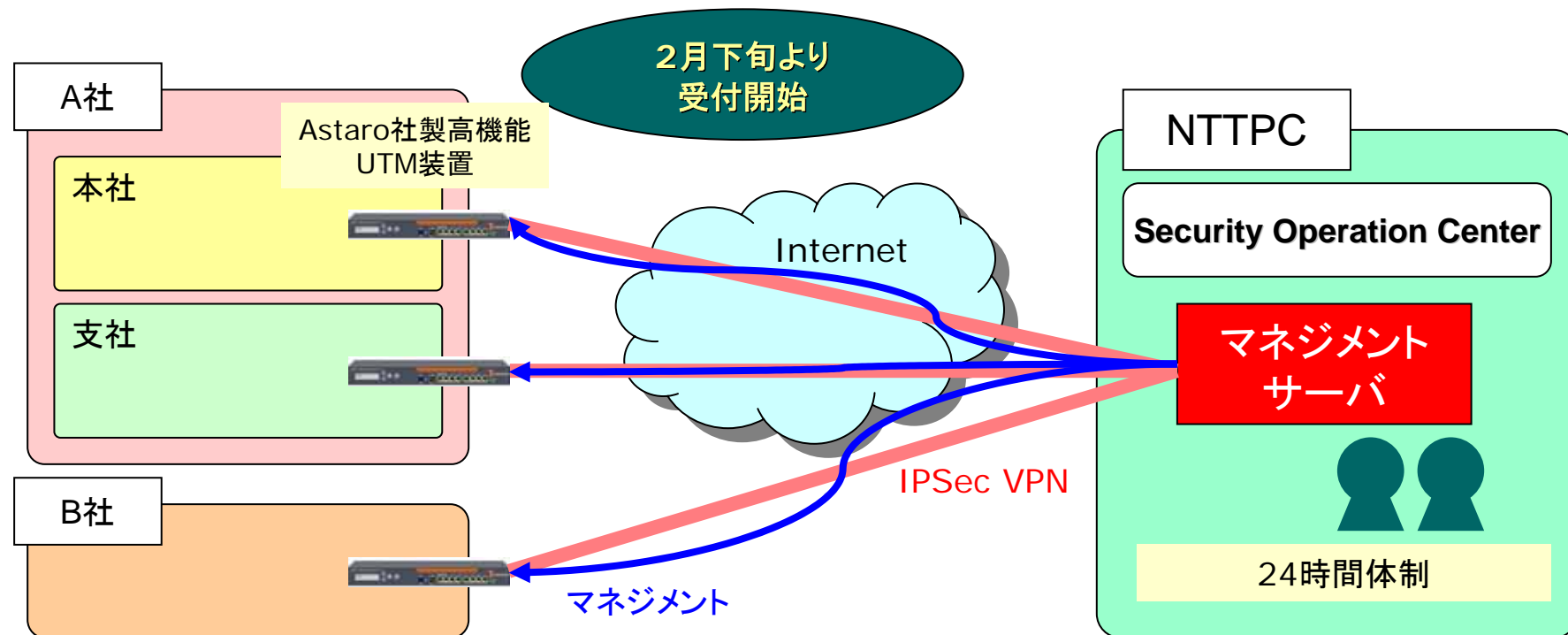


7-2. ゲートウェイ・セキュリティ運用監視サービス

Gateway Security Management Service

ゲートウェイ・セキュリティ運用監視サービスは、お客様の宅内に設置したゲートウェイ・セキュリティ装置の運用と監視を、NTTPCのSOC(Security Operation Center)から提供するサービスです。このサービスを導入することで、インターネット境界に対する幅広いセキュリティ対策を提供します。

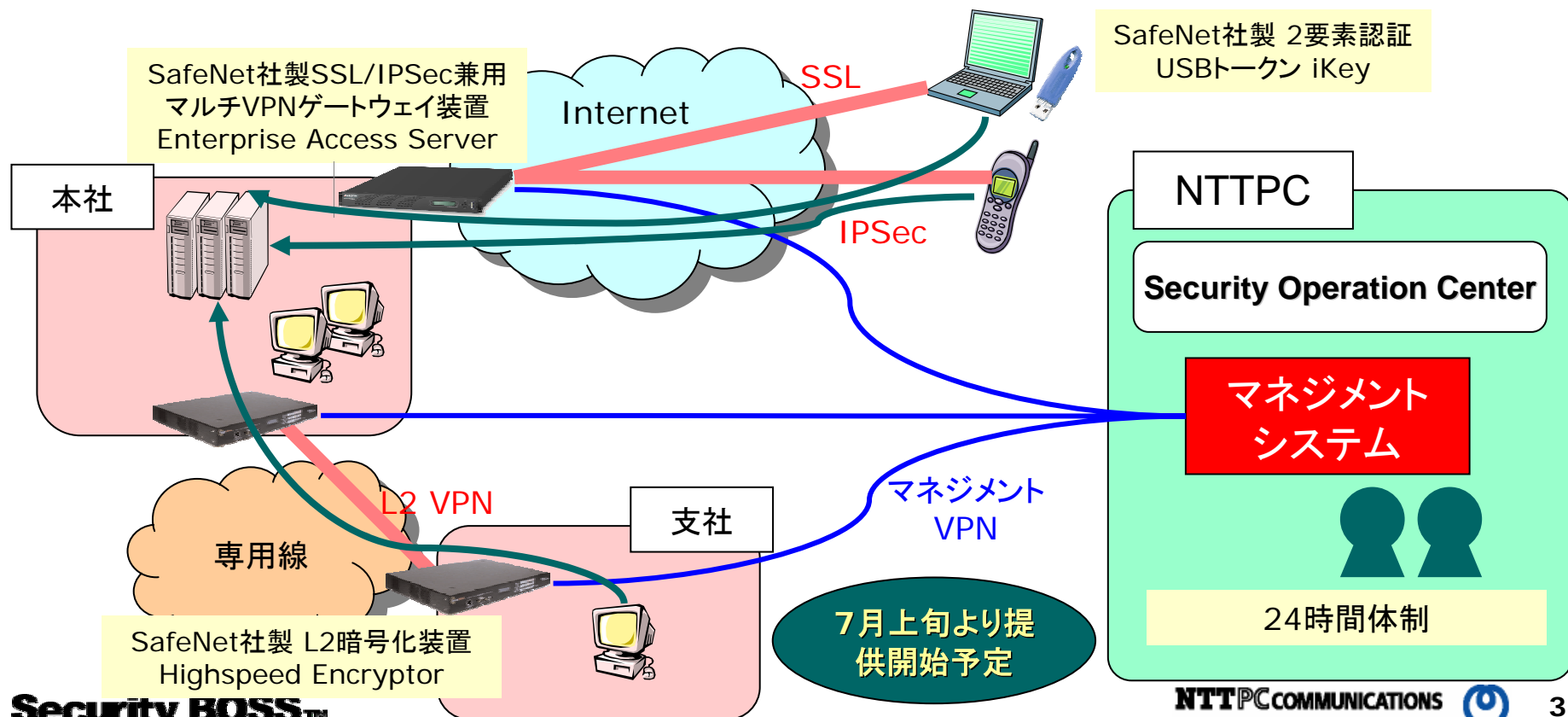
* 当社はインターネットVPN経由で行います



7-3. 通信暗号化運用サービス

Communication Encryption Management Service

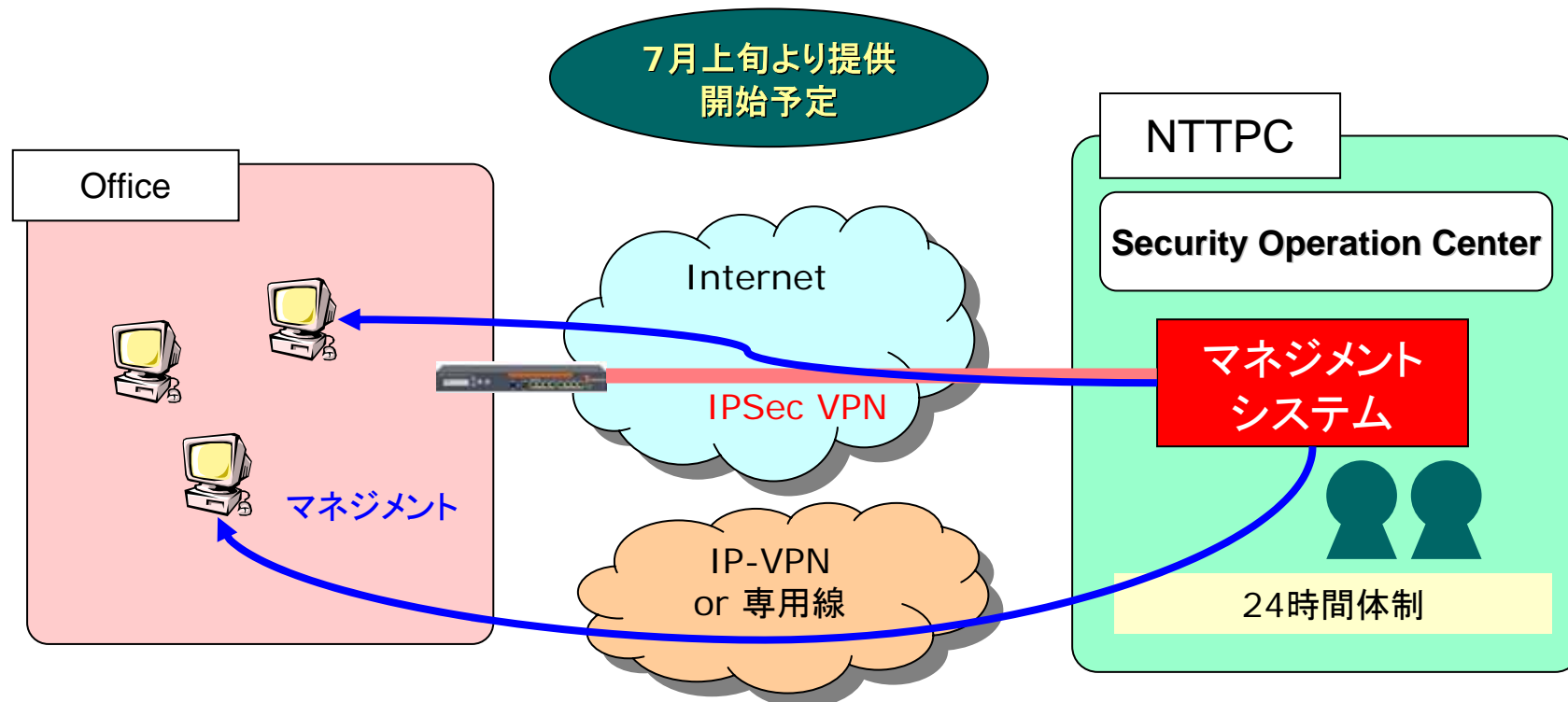
インターネット経由のSSL、IPSecを利用したVPN、および最近再び金融機関でも注目されている、専用線の暗号化をNTTPCのSOCで一元管理、運用するサービスです。このサービスを利用することで、お客様の通信の安全を確保することができます。



7-4. PCセキュリティ運用サービス

PC Security Management Service

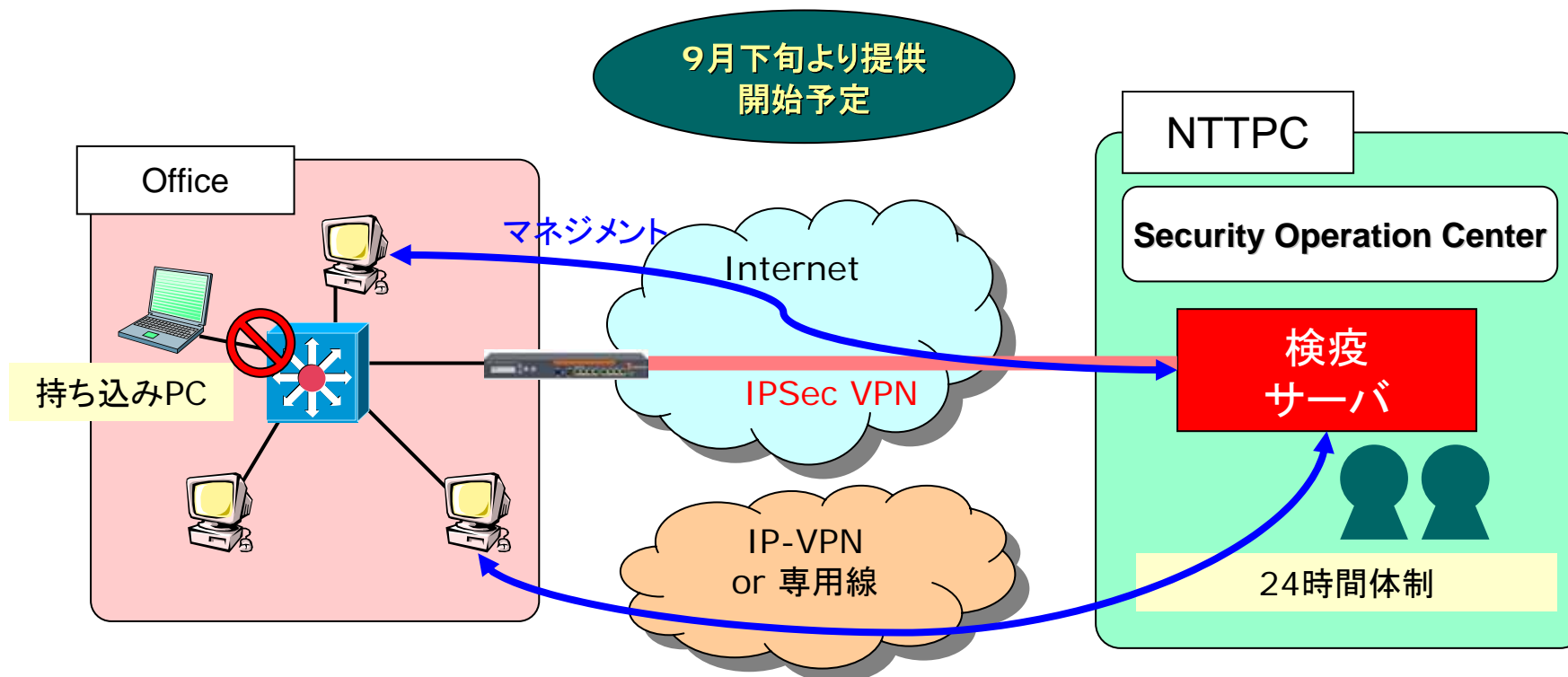
社内PCのパッチ適用状況、アンチ・ウィルスのシグネチャ・バージョンなどを、お客様のセキュリティ・ポリシーに基づいて、NTTPCのSOCから一元管理、運用します。このサービスを利用することで、煩雑な社内のPC管理を安全にアウトソースできます。



7-5. 検疫運用サービス

Quarantine Network Management Service

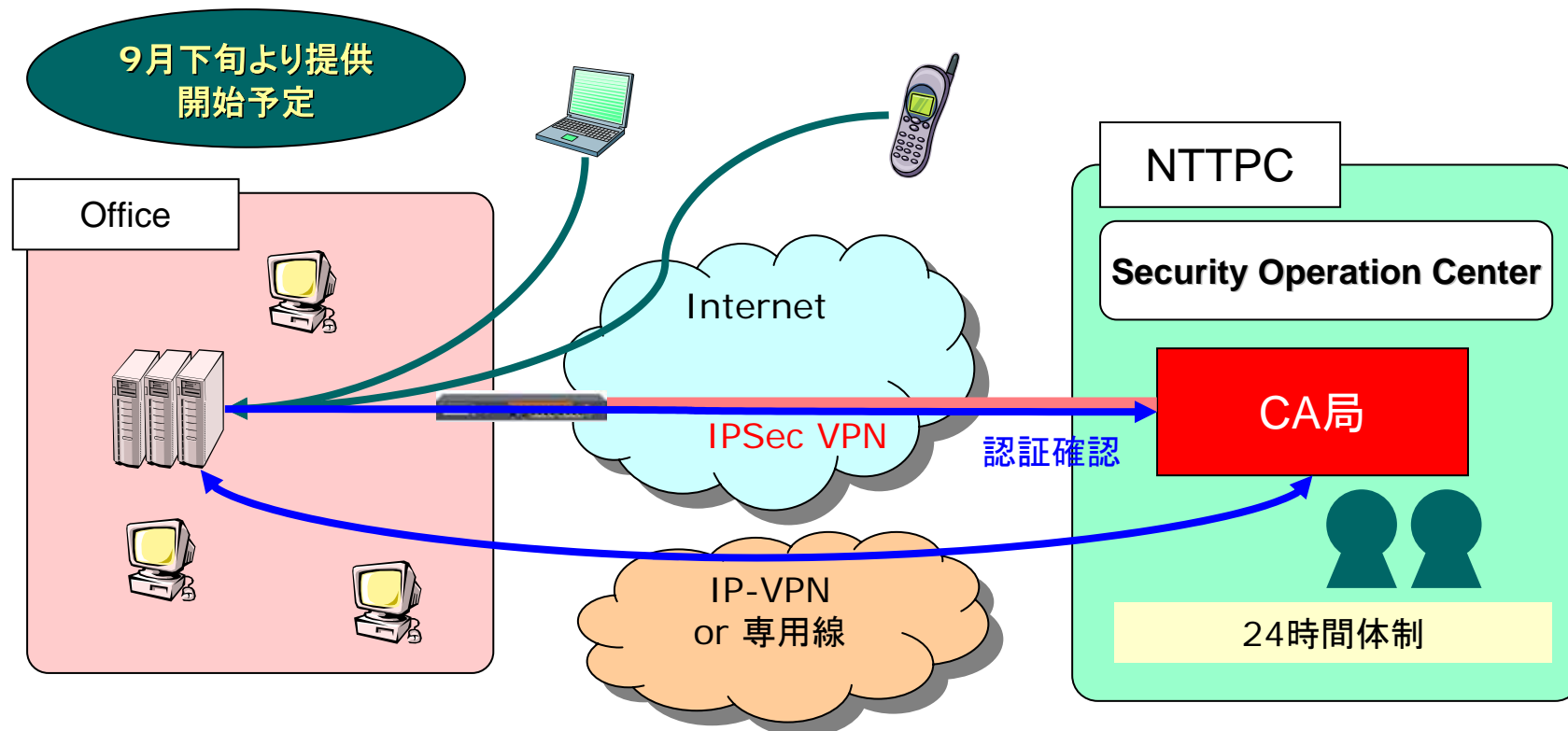
いわゆる検疫ネットワークの運用を提供します。このサービスを利用することで、社内のセキュリティ・ポリシーに違反している端末や、社外からの持ち込み端末をオフィス・ネットワークに接続させることを拒否したり、ポリシーに準拠するように強制したりすることができます。



7-6. PKI運用サービス

PKI Management Service

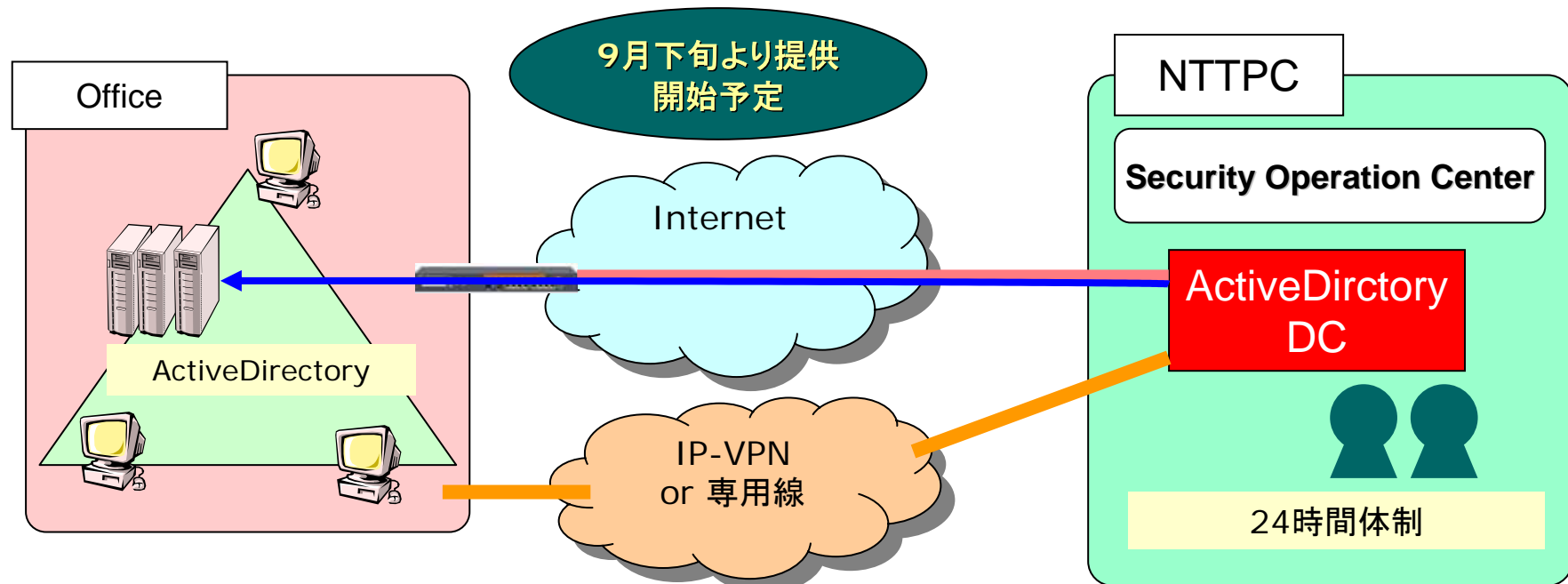
プライベートやグローバルのCA局の運用や電子証明書の発行/配布業務の代行をするサービスです。このサービスを利用すると、煩雑なCA局の管理や電子証明書の配布業務を安全にアウトソースでき、様々なアプリケーションの認証を強化することが可能になります。



7-7. ActiveDirectory運用サービス

ActiveDirectory Management Service

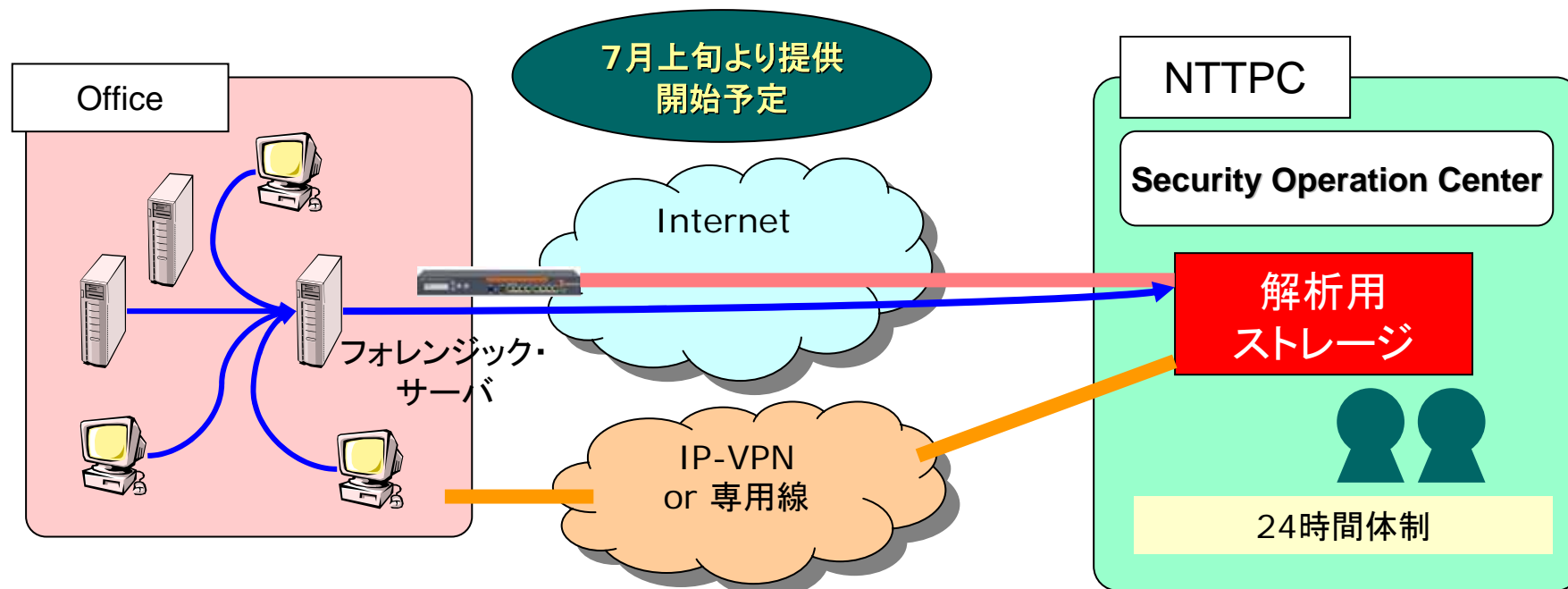
お客様のドメイン・コントローラの冗長サーバをNTTPC SOC内にホスティングし、そのサーバを利用して、お客様のActiveDirectoryを運用するサービスです。このサービスを利用すると、日々の煩雑なアカウント管理を安全にアウトソースすることが可能です。また、通信暗号化運用サービスやPKI運用サービスと組み合わせることによって、より安全でシングル・サイン・オン可能なリモート・アクセス環境も利用可能になります。



7-8. フォレンジック・サービス

Forensic Service

お客様社内の端末およびサーバのログや通信情報をフォレンジック・サーバに集め、定期的にNTTPC SOC内の解析用ストレージに収集して、有事の際に内容を解析し、実際に何が起こっていたのかを明らかにするサービスです。このサービスを利用することで、有事の際の対応をスムーズに行うことが可能となります。また、SOX法のモニタリング要素を強力にサポートするツールとしてもご利用いただけます。



7-9. システム診断サービスの概要

System Vulnerability Assessment Service

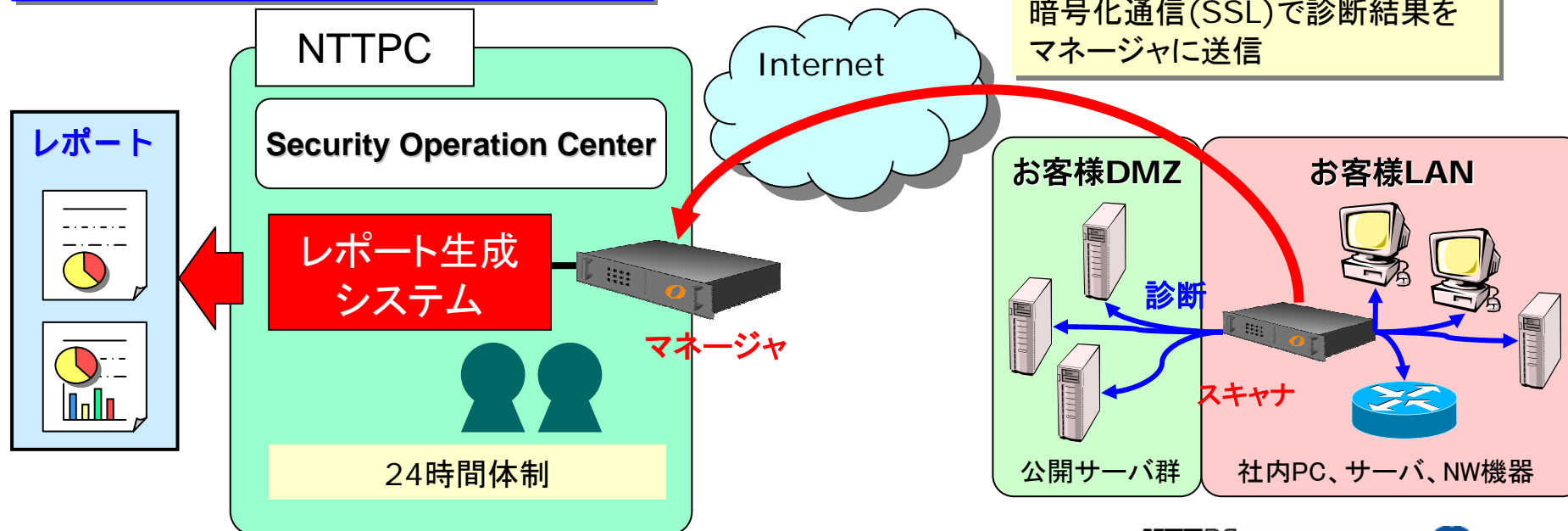
システム診断サービスは、弊社データセンターまたはお客様宅内に設置したスキャン装置(スキャナ)から、お客様のLAN内およびDMZにあるPCやサーバ、ネットワーク機器の持つ脆弱性を定期的に診断し、レポートします。

社内で抱える脆弱性の変遷を把握し、セキュリティ・レベルの管理に役立てることができ、SOX法で重要となるモニタリングを強力にサポートします。

nCircle社製脆弱性管理システム及び弊社開発のツールを使用してレポートを生成

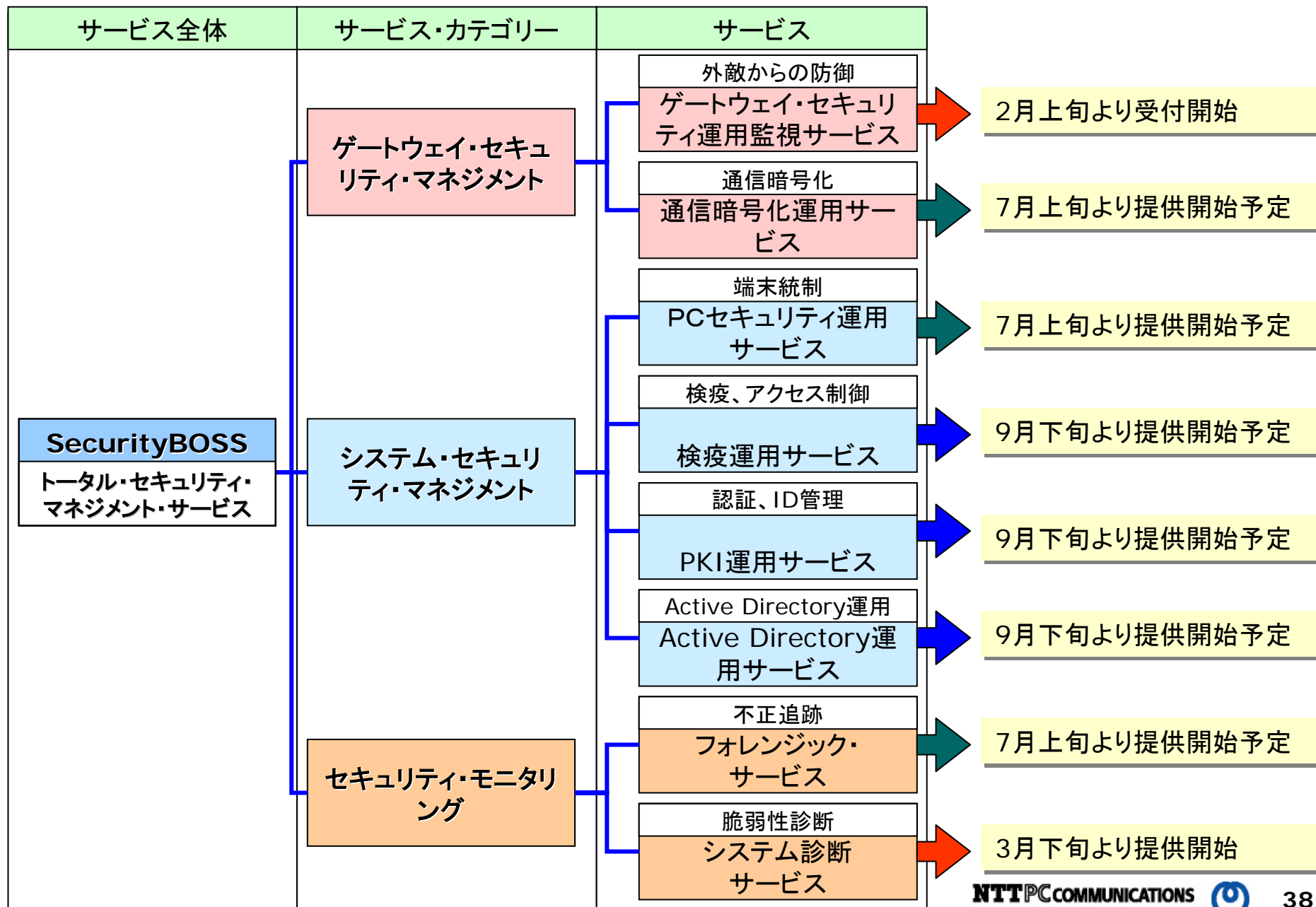
3月下旬リリース予定

暗号化通信(SSL)で診断結果をマネージャに送信



8. まとめ

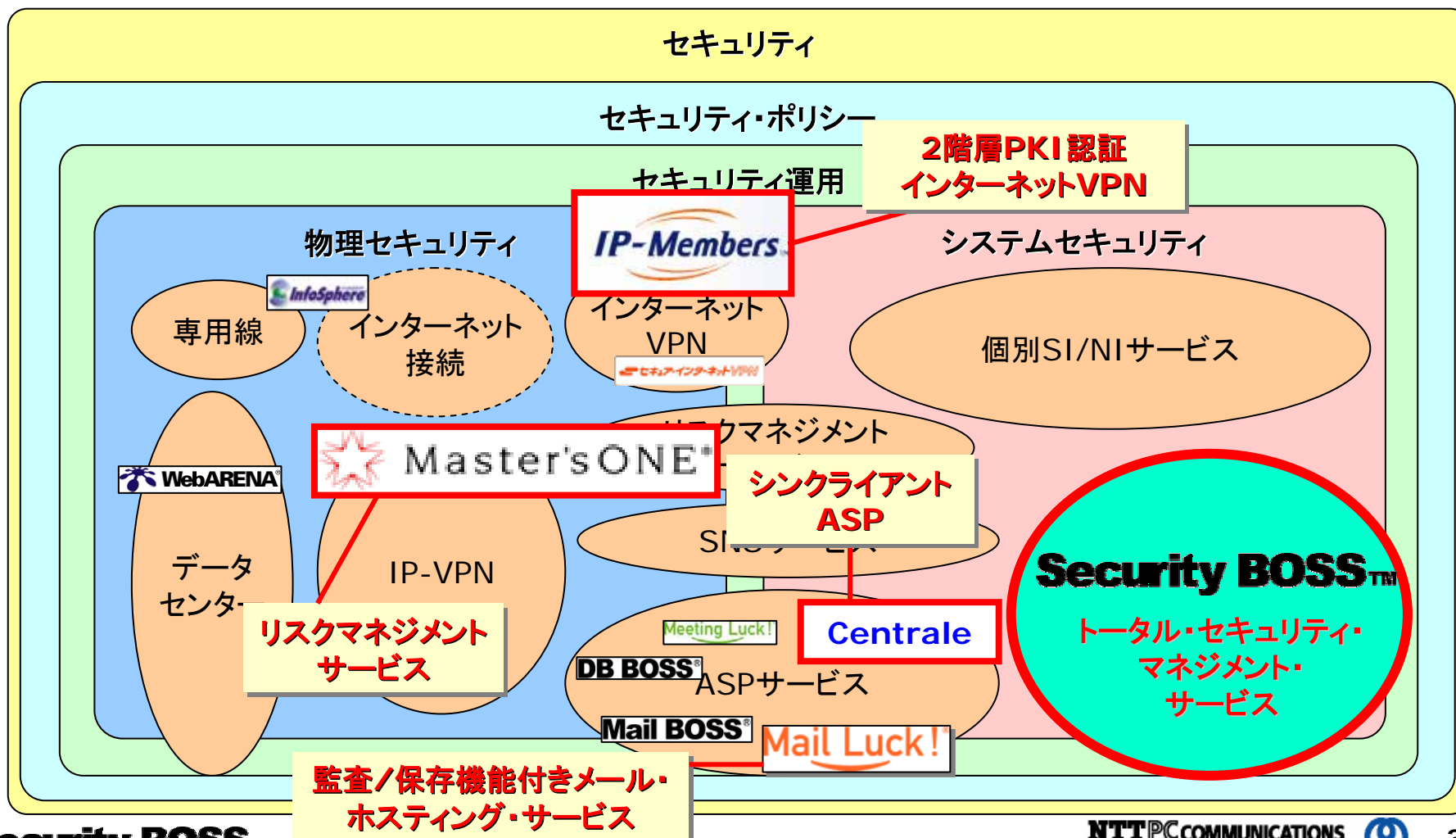
8-1. ロードマップ



8-2. NTTPCのセキュリティ・ソリューション・マップ

セキュリティ対策全般のカバレッジ

SecurityBOSSの提供開始により、NTTPCのセキュリティ・ソリューションはより完全に近い形でITセキュリティーをサポートできるようになりました



8-3. まとめ

コンプライアンスを意識したこれからのセキュリティ対策

アウトソース志向

信頼できる所にアウトソースすることで、コストを極小化する

サービス志向

汎用的に対応できるIT基盤部分はサービスを利用することでより安価にすませることが可能

オールインワン志向

専用線、VPN、インターネット接続、iDC、ASPサービス、セキュリティ・サービス、そして個別のNI/SIと、全てが揃っているからこそ、ポリシー策定時から運用まで、高いセキュリティを保ちながら一貫したコスト削減を実現できる



それがNTTPCのセキュリティ・ソリューション

Thank You!

お問い合わせ先

株式会社NTTPCコミュニケーションズ

オンデマンド事業部 インフォメーションセンター

(SecurityBOSS問合せ窓口)

TEL:03-3432-1330 E-mail:sec-boss@nttpc.co.jp

URL:<http://www.securityboss.jp>

※ 本文に記載されている会社名、サービス名、商品名は各社の商標または商標登録です。