SCSK GROUP

新しい
情報セキュリティ
リスクに
どう立ち向かうか

～ 今企業に求められる現実解 ～

2011年12月6日

株式会社JIEC
製品ソリューション推進室

目次

- ■　今なぜ再点検が必要なのか
  - □　使うリスクから使わないリスクへ
- ■　再点検時に留意すべきポイント
  - □　4つのステップと落とし穴
- ■　新技術・製品トレンドと導入の要諦
  - □　実効性・費用対効果を考えた現実解
- ■　ピンポイントソリューション徹底活用
  - □　サービス連携による対策強化
- ■　まとめ
  - □　本日ご紹介したサービスについて

■今なぜ再点検が必要なのか
□使うリスクから使わないリスクへ

使うリスクから
使わないリスクへ

◆ 200X年：コンプライアンス偏重の時代
　個人情報保護法、SOX法の施行
　「リスクがあるものは使わせない」風潮

◆ 201X年：変化への対応が求められる時代
　企業価値向上につながる技術の登場
　「使わないこと」が競争力低下のリスクへ

企業の内部情報は
企業の外部に存在

◆ クラウドコンピューティング
　サービス提供者への情報委託

◆ モバイル（外部）アクセス
　情報の外部持ち出し（複製、キャッシュ）

企業情報システムを取り巻く環境の変化（技術/価値観）

セキュリティリスク再点検の必要性

■再点検時に留意すべきポイント
□4つのステップと落とし穴

再点検4つのステップ

STEP-1

現状把握
（セキュリティマップなどのツールによる可視化）

STEP-2

対応すべきリスクの明確化
（“3つのリスク”と“リスクを引き起こすリスク”）

STEP-3

リスク対策の切り分け
（リスク管理の3つの構成要素）

STEP-4

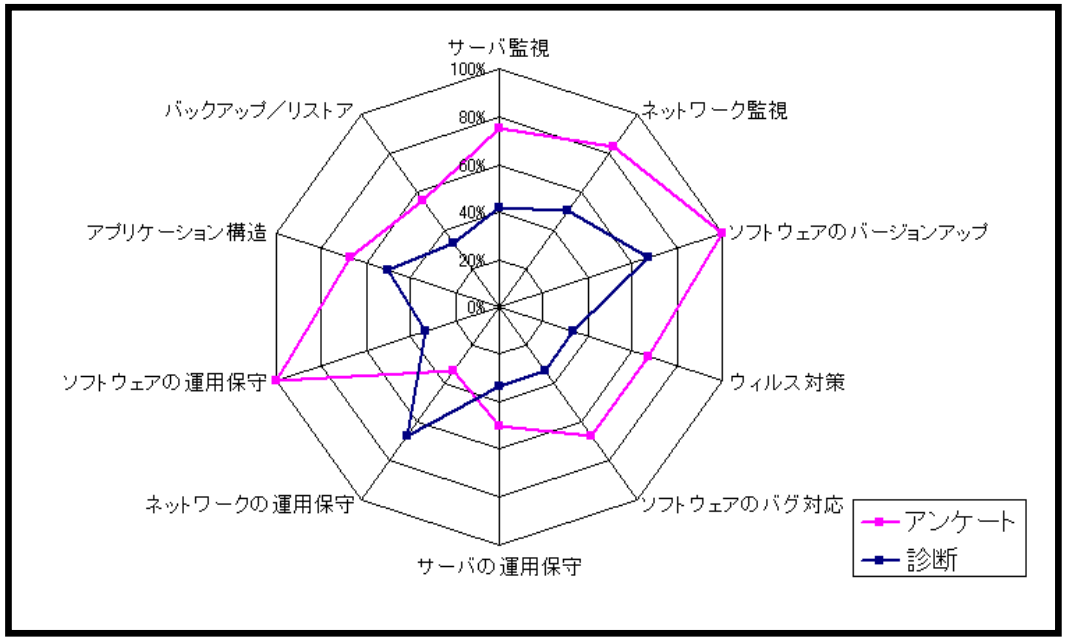
技術的対応方針策定
（リスク発生箇所と対応箇所の違い）

STEP-1 現状把握

IT投資分析手法の応用

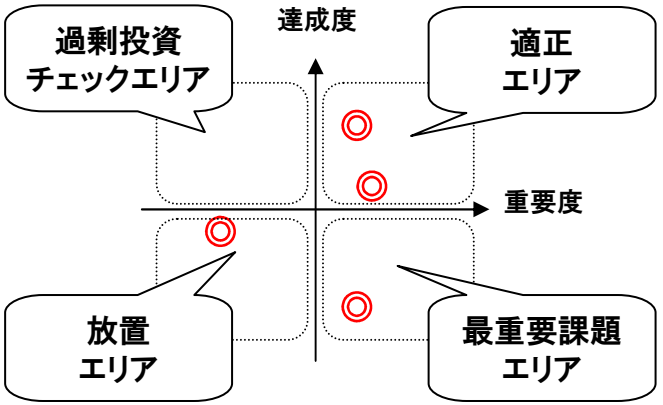
◆ 当社の独自方法論『ITライフラインクリニック』による評価例

信頼性の評価例

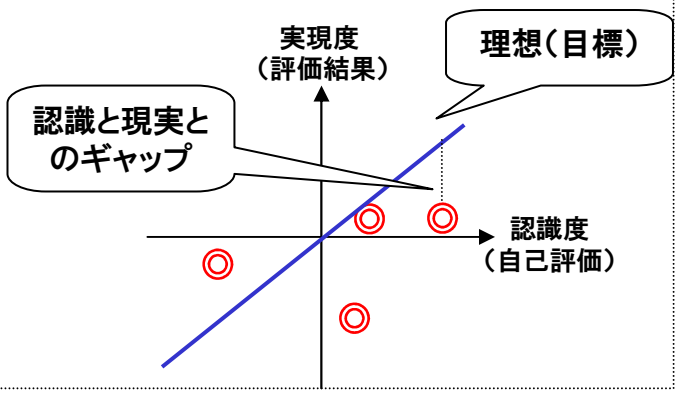


実態（実査）と認識（アンケート）の比較で
セキュリティ対策の全体像を把握

重要度×達成度分析



認識度×実現度分析



STEP-1 現状把握

セキュリティマップによる対策状況の可視化

講演でご紹介いたします

セキュリティマップ上に、導入済みの製品・サービスをプロットすることで
自社のセキュリティ対策状況を可視化して把握することが可能に。

STEP-2 対応すべきリスクの明確化

＜3つの本質的なリスク＞

IPA定義を参考に独自定義

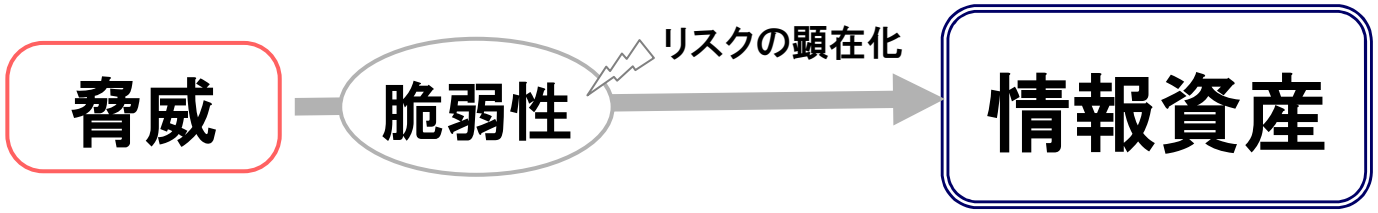
『情報漏えい』、『サービス停止』、『改ざん』

（＋）4つのリスクを引き起こすリスク

なりすまし、盗聴、不正アクセス、ウィルス侵入

＜リスク・脅威・脆弱性の考え方＞

JIS Q27002:2006(ISO/IEC 17799:2005) を参考に記述



脅威に対し脆弱性が存在するとき、初めてリスクは顕在化する。

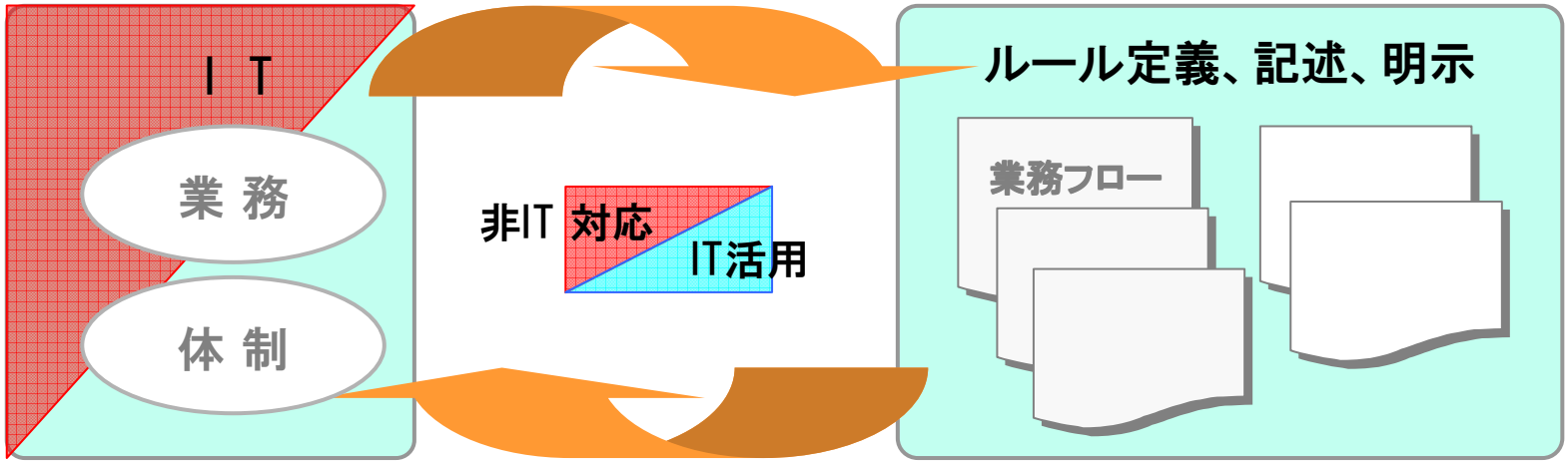
情報資産	組織にとって価値のある情報および情報処理施設、関連資産。 （情報／データ、ハード、ソフト、インフラ、文書など）
脅威	情報資産に対し損害を与える可能性のある潜在的な原因。 （悪意によるものと、天災や故障など作為的でないものを含む）
脆弱性	脅威に対して 情報資産が持つ弱点。 （欠陥などシステム上の問題や、体制など人間の行動に関する問題を含む）

STEP-3 リスク対策の切り分け

＜リスク管理の3つの構成要素＞

『テクノロジー』、『コンプライアンス』、『マネジメント』

IT活用　　非IT対応

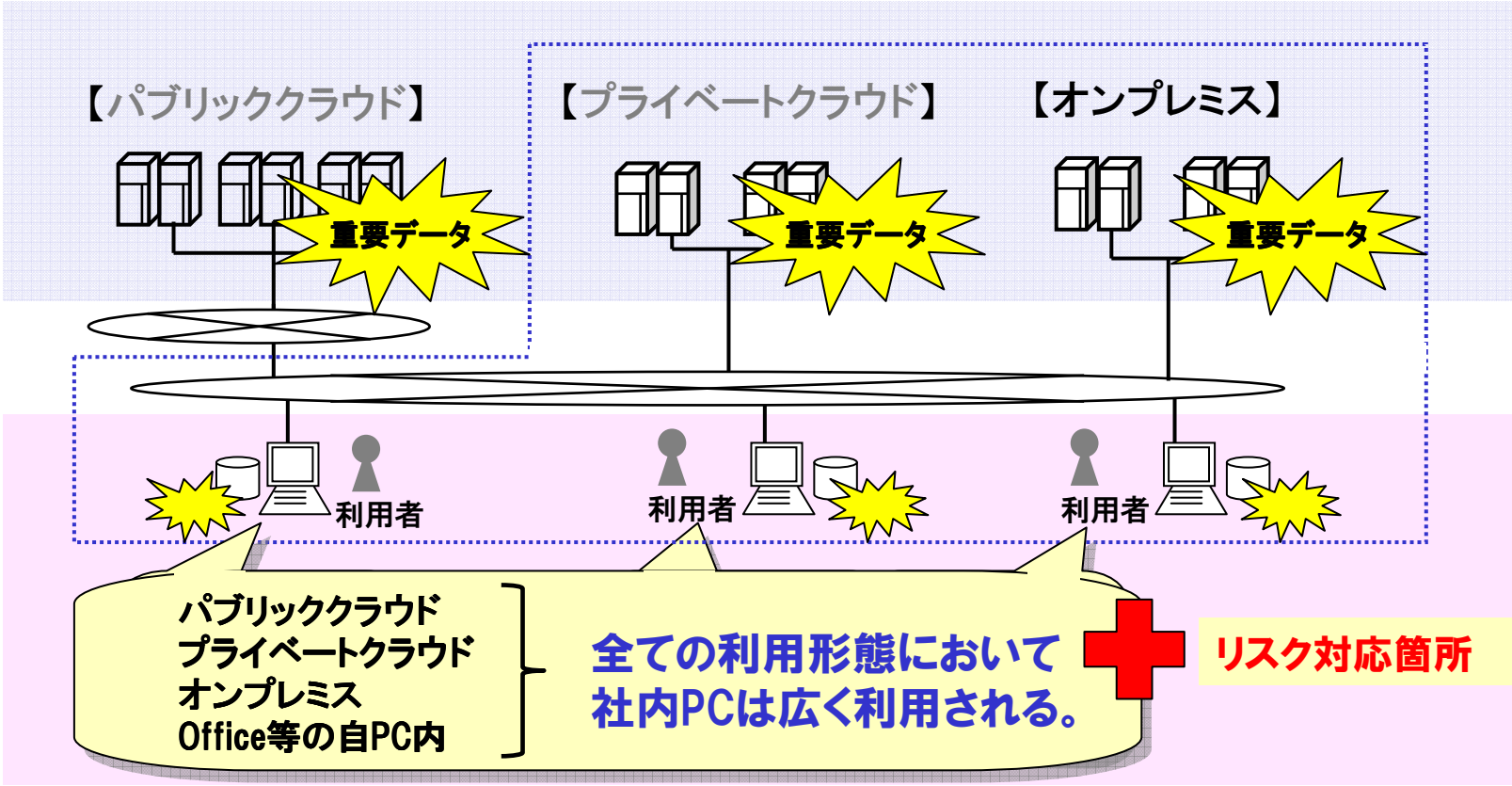


セキュリティ、リスク管理に関する考え方の基礎は
システムを取り巻く背景が変わっても適用可能

STEP-4 技術的対応方針の策定

＜リスク発生箇所とリスク対応箇所の違い＞

同種のリスク対応は集約した方が、効率的であり一貫性も保てる。



社内外に偏在するシステム・データとユーザとの接点となる端末サイドは、
複数個所で発生するリスクに対応する必要があるポイントの一つである。

■新技術・製品トレンドと導入の要諦
□実効性・費用対効果を考えた現実解

情報セキュリティトレンド解読

■情報セキュリティトレンドに新たに追加すべきテクノロジ

講演でご紹介します

■上記から読み取れるトレンド

◇[　　]に対するセキュリティに注目⇒1,2

◇従来の総合的ソリューションの[　　]

⇒2([　　]),3[　　]

◇[　　]に対する[　　]

⇒2,3,4

新技術・新製品導入検討の要諦

■統合型か、特化型か

対応すべきリスクの定義によって答えは異なる。

・潜在リスクを含む広範囲な対応を検討している場合
⇒それらのリスクを総合的にカバーする技術・製品が存在する場合、『統合型』ソリューション導入は一考に値する。

・顕在化している単一リスクへの対応を検討している場合
⇒統合型のソリューションよりも、対処すべき顕在リスクの対策に特化したピンポイント型ソリューションの採用が、即効性、コスト、導入スピードの面で最適解になり得る。

再点検4つのステップで述べたとおり、対応すべきリスクの定義が第一歩。
定義したリスクに対応する技術・製品ジャンルの判断には、
現状把握に使ったセキュリティマップなどの可視化ツールが有効。

総合型・特化型の特徴比較

■コスト・難易度高い総合型、網羅性・転用性低い特化型

統合型＞特化型	統合型＜特化型	統合型？特化型
網羅性 転用性	導入コスト（初期） 導入スピード 難易度	費用対効果 実効性

統合型製品を適切に機能させ、導入効果を高めるためには、正確なセキュリティ対策の現状理解と製品理解に基づく、計画的アプローチが必要であり、それには一定の時間と投資（コスト）を要する。
このプロセスを軽視して統合型製品を導入しても、対応範囲の広さが仇になり、どのリスクに対しても不十分な対策となってしまうことがある。

＜総合型を選択する場合のその他の考慮点＞

・多くの製品がスイート化（多機能化）を志向しており、同等または類似機能を有する製品が多いため、製品ジャンル選定、製品選定の見極めが困難。
・導入済み製品や既存の仕組みとの重複に注意。過剰投資となる可能性があるだけではなく、ポリシー矛盾等で運用に混乱をきたすと新たなリスクが生じることもある。

総合型・特化型の特徴比較

■特化型ピンポイントソリューションの薦め

統合型＞特化型	統合型＜特化型	統合型？特化型
網羅性	導入コスト（初期） 導入スピード 難易度 転用性（解約可能）	費用対効果 実効性

網羅性を除いて、
『特化型×利用型』
に軍配

＜特化型の欠点を補う『サービス提供』方式＞

・特化型の欠点は、ピンポイントであるが故に対象となっているリスクが何らかの理由で解消されるなど、外部環境が変化した場合に転用がきかない点。
『サービス提供』方式（利用型）のソリューションの場合、不要になればいつでも利用を停止することが出来る上に、導入コスト・スピード・難易度の面でもメリットが強化される。

対応すべき課題が単一かつ明確な場合は、
実効性・コストの両面から
【利用型ピンポイントソリューション】の採用が現実解となる。

情報漏えいリスクへのピンポイント対策紹介

- 3つの本質的リスクの一つである『情報漏えい』に対する利用型ピンポイントソリューション

■対応すべき顕在リスク：PCからの情報漏えい

⇒ 情報漏えい対策　モニタリング・サービス

■対応すべき顕在リスク：メールによる情報漏えい

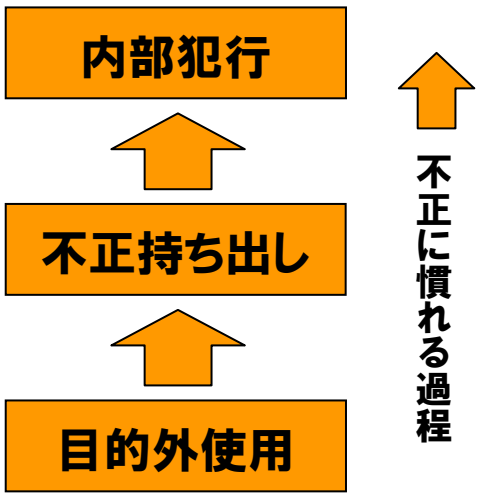
⇒ PlayBackMail Online

PCからの情報漏えいリスク対策

■情報漏えいの顕在化するポイントと不正に慣れる過程

情報漏えいが犯行まで至るかどうかは、不正に持ち出された情報がどう扱われるか
次第であり、ITで対応するリスクとすべきなのは『不正持ち出し』の発生を防ぐこと。
また不正が日常化しないように、抑止の観点で目的外使用を規制することも必要。

今の仕事で得たノウハウ情報を持ち帰った。 転職先へのおみやげとして、製品情報を持ち帰った。 転売目的で、機密情報を盗み出した。
業務情報を持ち帰り、自宅で作業し週明けに戻した。 自分が開拓した顧客のデータを持ち帰った。 自分が担当した新製品情報を記念に持ち帰った。
会社のPCでゴルフのスコアを管理している。 学生時代の友達に、同窓会のメールを送った。 ネット銀行でプライベートの振込みをした。



「あやしい行動(不正では無く不正に繋がる行為)」を早期に発見・是正する
事で、「犯罪発生を未然に把握」、「抑止効果が期待」につながる。

PCからの情報漏えいリスク対策

■不正と不審に対応する「情報漏えい対策 モニタリング・サービス」

不正な操作の検知と防止

端末監視ソフトウェアによる
不正操作の防止

不審な操作の把握と原因追及

ログ統合・証跡管理SaaS「Log Shelter」
による操作ログの分析

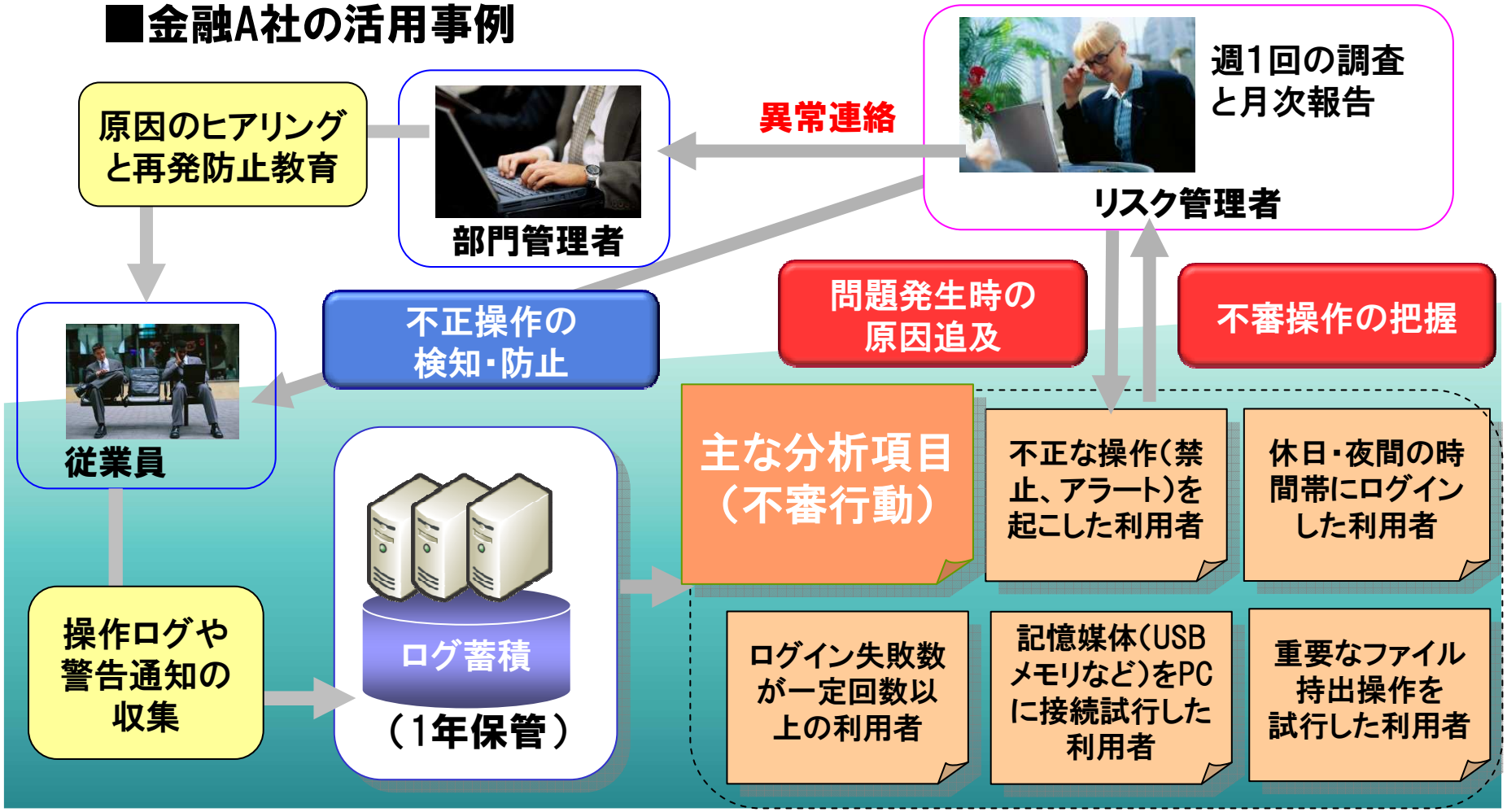
「不正な操作の検知と防止」と、「不審な操作の把握と原因追及」
をバランスよく行うことで、ユーザに負担のかからない
情報漏えい対策が可能となります。

情報漏えい対策の現実的かつ完全な選択肢
情報漏えい対策ソリューション

情報漏えい対策 モニタリング・サービス

PCからの情報漏えいリスク対策

■金融A社の活用事例



日々の監査作業の実施により大きな犯罪を未然に防ぐことが可能

PCからの情報漏えいリスク対策

■追加提供予定機能

定期的な調査作業負荷、不審行動のノウハウ不足、調査迄の確認の遅れなどがリスク対策上の課題となっていた。

不審操作通知機能　（提供予定）

予め用意された不審（あやしい）操作を検知し、管理者にメール通知。管理者は通知内容を確認することで、効率的にリスクを把握し、詳細調査・対応することが可能となる。

期待効果

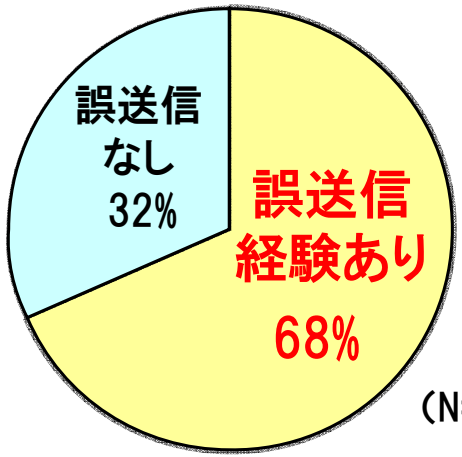
- 定型調査作業の軽減（ルーチンワークからの解放）
- 不審行動の早期発見（初動スピード向上）
- 見過ごしリスクの低減（不審行動のノウハウ向上）

メールによる情報漏えいリスク対策

■メール誤送信の現状

- ◆就業者の7割がメールの誤送信の経験あり
- ◆誤送信経験者の約2割は、自分で誰にも報告していない

Q.メール誤送信の経験があるか？



(N=4,884)

Q. 誤送信の事実をどのように報告、連絡したか？

自分で会社、組織に報告・連絡	51
自分で顧客、取引先に報告・連絡	35
自分では誰にも報告・連絡していない	19
自分で連絡しなかったが、他から会社や取引先へ連絡があった	8

(N=100 複数回答)

出展:NPO 日本ネットワークセキュリティ協会
『情報セキュリティインシデントに関する調査報告書～発生確率編～ 』を参考

⇒表面化していなくてもメール誤送信による事故は既に発生している可能性がある

メールによる情報漏えいリスク対策

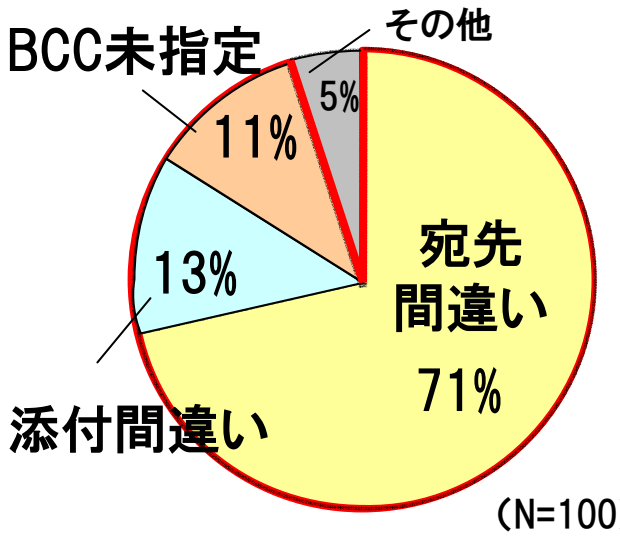
■メール誤送信の原因と対策案

◆誤送信の原因は主に3点

①宛先間違い

②添付間違い

③BCC未指定



出展:NPO 日本ネットワークセキュリティ協会
『情報セキュリティインシデントに関する調査報告書
～発生確率編～ 』を参考

宛先間違い・件名・本文の
書き間違いをした場合も
送信保留でやり直し可能

添付ファイルを間違えて
送ってしまった場合も
**添付ファイルを自動暗号化
パスワードを別途送付**

TO,CCに大量のアドレスを
指定した場合も
BCCに自動変換

メールによる情報漏えいリスク対策

■メール誤送信対策の事例

講演でご紹介いたします

メール誤送信防止サービス「PlayBackMail Online」

■メール誤送信防止サービス「PlayBackMail Online」

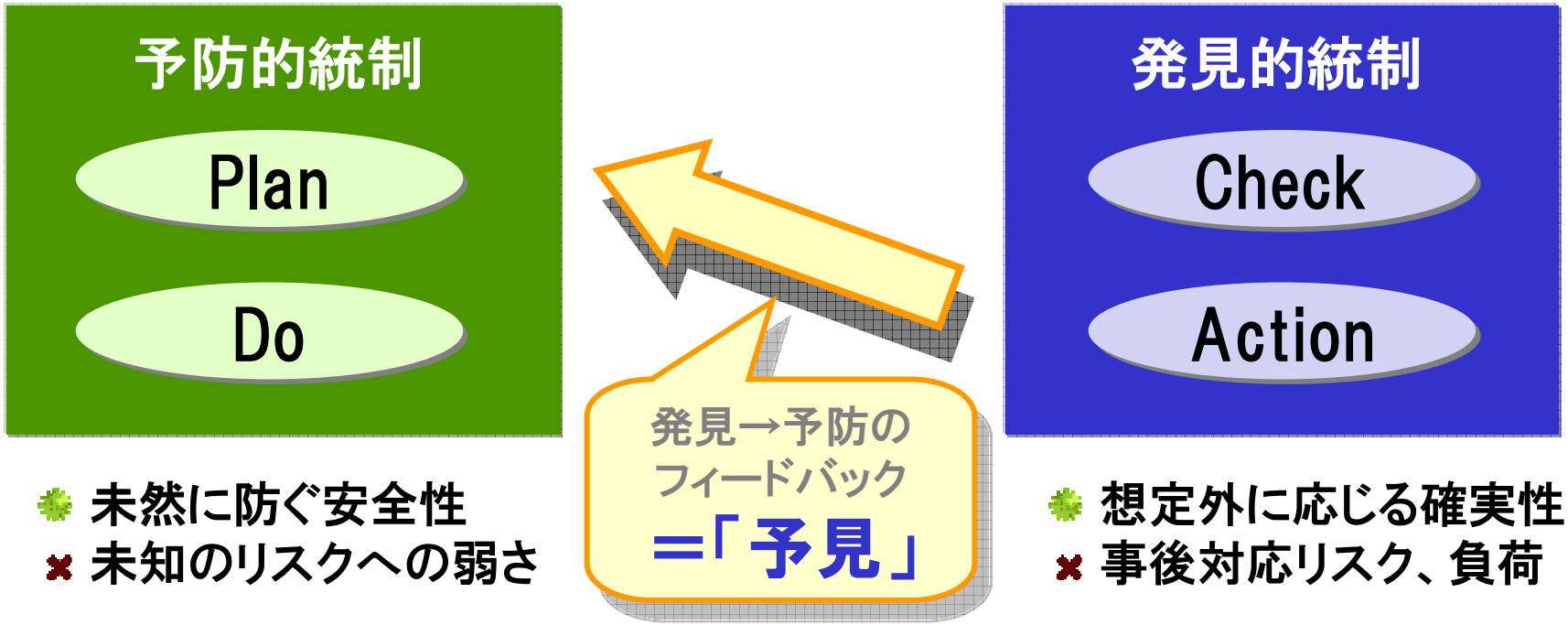
- ◆現場の業務効率を落とさずに導入可能
- ◆クライアント アプリケーションの導入が不要
- ◆属人的な防止策から、組織で統一した防止策へ
- ◆スマートフォン(iPhone)からも利用可能
- ◆Microsoft Office 365 Exchange Online/ Google Apps Gmailに対応

3つの機能で、メールの誤送信を強力に防ぐ

メール送信の保留	第3者確認・上長承認	暗号化・Bcc 変換
メール送信を一定時間保留。問題点に後から気付いた時にも送信を取り消せます。	宛先に含まれた社内の受信者に先行してメール送信、問題点に気付いた場合、送信を取り消せます。	添付ファイルの暗号化処理や宛先のアドレス情報を変換します。

■ピンポイントソリューション徹底活用
□サービス連携による対策強化

内部統制観点から見たリスク管理のポイント

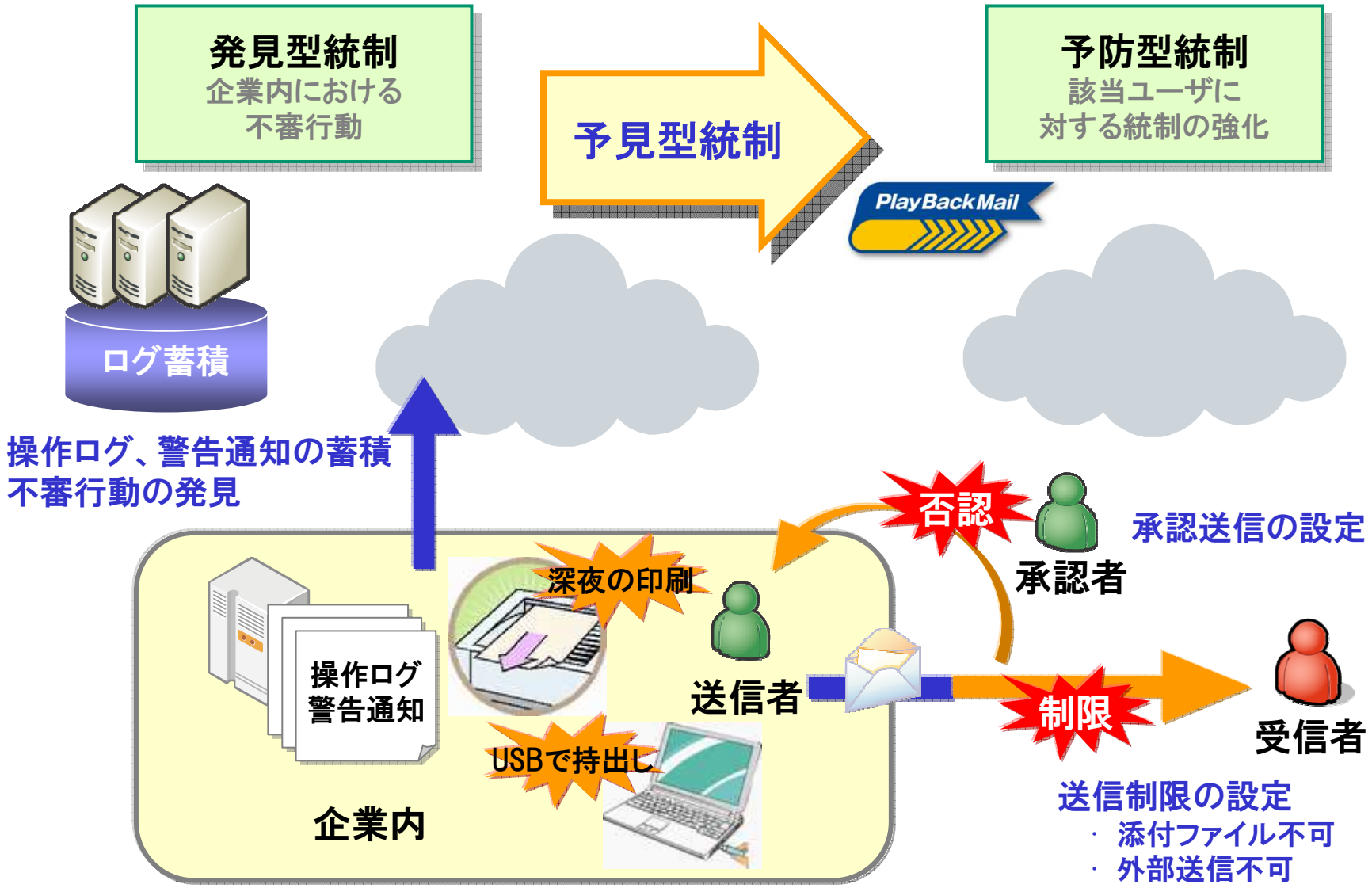


- ✿ 未然に防ぐ安全性
- ✖ 未知のリスクへの弱さ

- ✿ 想定外に応じる確実性
- ✖ 事後対応リスク、負荷

発見的統制と予防的統制を橋渡しすることで、
双方の弱みを補い合うリスク管理が可能になる。

クラウドサービス連携による予見型統制の例



■まとめ
□本日ご紹介したサービスについて

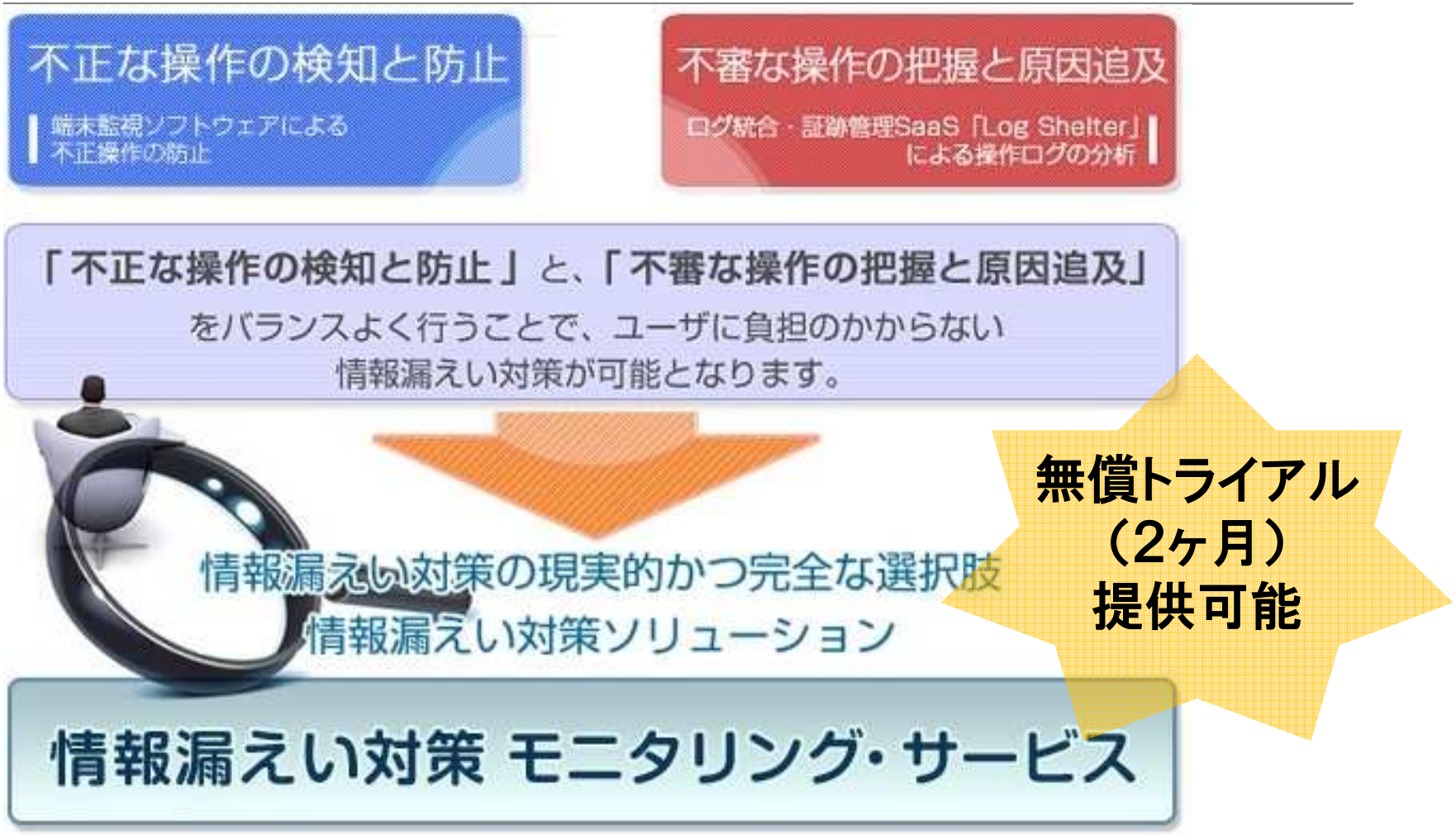
本日のまとめ

- セキュリティリスク再点検のツボ
  - セキュリティマップによる対策状況の可視化と弱点の把握
  - “本質的なリスク”と“リスクを引き起こすリスク”の見極め
  - リスク対策の整理(テクノロジ/コンプライアンス/マネジメント)
  - 具体的対策実施

- 情報セキュリティトレンドと新技術・製品導入の心得
  - 従来製品の特定機能に対応するスペシフィックな特化型製品の登場
  - 統合型ソリューション導入の課題は、
    機能重複(過剰投資)、運用負荷(整合性維持)、導入難易度
  - 個別の新しいリスクにピンポイントで対応するソリューションの有用性
  - 利用型×ピンポイントで即効、低コスト、スピード導入が可能に

- 情報漏えいリスクに対応するSCSKの利用型ピンポイントソリューション
  - 情報漏えい対策　モニタリング・サービス
  - PlayBackMail Online
  - サービス連携による組み合わせで生まれる新たな可能性
    ・予防型対策と発見型対策の短所を相互補完する『予見型』ソリューション

まとめ：本セッションでご紹介したサービス



1端末あたり　700円／月

詳しくはWebページへ　http://jiec-leakage.scsk-sol.jp/

まとめ：本セッションでご紹介したサービス

うっかりミス は防げないと思っていませんか？！

ユーザーが負担が少ない
電子メール誤送信防止サービス

PlayBackMail

3つの機能で、メールの誤送信を強力に防ぐ！

30日間
無料トライアル
提供可能

1ユーザーあたり　150円／月

詳しくはWebページへ　http://www.playbackmail.com/

SCSK GROUP

住商情報システムとCSKは、2011年10月1日をもちまして合併し、「SCSK株式会社」として、新たな一歩を踏み出しました。国内22社、海外7社のSCSKグループ各社の総力を結集して、お客様の競争優位を生み出すサービスをご提供します。

※本資料でご紹介のサービスは、SCSKグループのJIEC,CSK Winテクノロジが提供するサービスです。

お問合せ先

◆情報漏えい対策 モニタリングサービス

株式会社JIEC　製品ソリューション推進室

Mail: log_solution@jiec.co.jp

URL: http://jiec-leakage.scsk-sol.jp/

◆メール誤送信防止サービス　PlayBackMail Online

株式会社CSK Winテクノロジ

Mail: sales@cskwin.com

URL: http://www.playbackmail.com/