次世代の情報セキュリティ政策に関する研究会

資料4－2

5年後の情報セキュリティ

～　議論のネタを提供する　～

2008年1月31日

日本電気株式会社
第一システムソフトウェア事業部
則房雅也、CISSP

プレゼンテーションの構成

- ５年後の状況仮説（予測）
  - 企業、ユーザ（個人）、アプリケーション／業務システム、情報機器に関して
  - 社会状況、通信インフラ、などは含まれていない
- 状況仮説を背景にしたセキュリティ課題（予測）
  - 企業、ユーザ（個人）、アプリケーション／業務システム、情報機器に関わるセキュリティ
- 企業でのセキュリティ管理に対する施策（例）
  - 協調型セキュリティ
  - デモ

５年後の状況仮説１
（企業）

企業におけるプラットフォームセキュリティ管理
（プラットフォーム＝情報の器： PC、サーバ、ファイル、ネットワーク、装置）

- PC(エンドポイント)側セキュリティ対策はほぼ完了
  - ユーザ認証、PC暗号化、データIO制御、AV、P-FW、などが徹底
- NW側セキュリティ対策は検疫/NACの実装がほぼ完了
  - ネットワークアクセス時にユーザ認証が徹底
  - 安全な無線LANアクセス、リモートアクセスが定常化
- データセキュリティがますます重要
  - IRM/DRMが浸透、しかし組織を超えたアクセス権限管理は困難
- セキュリティ対策浸透の結果、積極的なIT利用形態に移行
  - PCやデータの持ち歩きが復活
- サーバ、ストレージのセキュリティ対策は予測困難
  - ログ管理はコンプライアンスを背景に浸透
- 新しいデバイスのセキュリティ対策は予測困難

企業におけるシステムセキュリティ管理
（システム＝情報を使うロジック： 業務システム、アプリケーション）

- ウェブ、メールのセキュリティは大幅改善、新しい課題も多発
- DBセキュリティも改善する
- 業務システム自身のセキュア化は進まない
  - プラットフォームのセキュリティ対策への依存大
  - セキュアプログラミングの浸透はすぐには進まない
    - プログラミング力が低下している、ソフトウェアエンジニアリングの停滞
    - 広範なセキュリティ知識の習得は困難、実践的習得機会が少ない
    - 投資対効果を明確に説明できないため取り組みが後手に回る
  - 個別対応で標準的な実現手法がないため非効率
- 新しいソフトウェア技術へのセキュリティ対策は予測困難
  - 業務システムの一部はSaaSへ移行、既存システムとSaaSのマッシュアップ化が進展

その他企業における状況

- その他のセキュリティ
  - ネットワークでエンド・ツー・エンドの暗号化が提供されると、既存のFW/IDS/IPSが効果を発揮しなくなる
  - ビル、居室などでのフィジカルセキュリティは浸透
    - フラッパーゲート、ICカード、監視カメラ、など
- セキュリティ管理体制
  - セキュリティ管理者数＜セキュリティ課題数
  - アウトソースと内部管理の両極化
    - 従来の方式(イベントドリブンなパッチワーク)は破綻
    - セキュリティ問題をさばける技術者の育成は困難
    - 高品質なセキュリティ管理サービスを提供するサービスベンダーは少ない
- キラーアプリケーション
  - やはりウェブとメールとMS Office
  - ブラウザ上で動作するリッチクライアントの更なる進化
  - いろいろなデバイスでIP電話の導入が進展

５年後の状況仮説２
（ユーザ）

ユーザの特徴

企業では、

- 契約社員、委託先社員、協業先社員が急増
  - 退職者の再活用、グローバルリソースの活用
  - 内部社員のモラル、モチベーション維持、技術力・知識強化が課題
  - モバイルワーカー、サテライトオフィス・テレワーカーの増加
- 吸収合併によるITシステム統合
  - 価値観の異なるユーザの共存
    - セキュリティポリシーの見直し、セキュリティ管理者の混乱、ユーザの混乱、セキュリティシステムの不整合

社会では、

- ITとインターネット利用者層の拡大
  - 主婦層、老齢者、地域へのユーザ拡大
  - セキュリティ管理を自力で行えないユーザがほとんど

個人の状況(自宅など)

- ネットワークアクセス主目的
  - 情報家電の宅外からの制御
  - 音楽、映画などのダウンロード
  - ショッピング、オークション
  - 銀行手続き、申告類、等の作業
  - 対戦型ゲーム、トーナメント
  - 生涯学習
- コンピューティング環境
  - PC、携帯、PDA、ゲーム端末、情報家電など、複数端末の保有と利用
  - 目的にあわせて使いやすい端末を利用
  - どの端末を使ってでもブロードバンド通信でインターネット利用が可
  - ほとんどのユーザはセキュリティを気にしない
- キラーアプリケーション
  - (予測困難)

５年後の状況仮説３
（企業・個人の周辺環境）

装置、サービス

- ネットワーク装置
  - セキュリティ機能の標準装備
  - ICT装置化（アプライアンスなど）
- コンピュータ
  - Virtual Machine（複数OS環境、それぞれでのアプリケーション利用）
  - シン・クライアント
- キラーサービス
  - 単機能・簡易サービスは携帯端末から
- ICTの活用
  - 介護・高齢化問題へのICTの活用
  - 子供の安全や教育に対するICTの活用
  - 環境問題へのICTの活用

状況仮説１に基づいた課題
（企業）

課題

セキュリティ管理の複雑さ

- セキュリティ管理が複雑になり管理上のミス多発
- 運用管理組織の縮小と管理対象の分散化により出現する無管理空間
- 新型vs旧型、ベンダーvsベンダーで、セキュリティ製品機能の互換性、管理一貫性が困難
- 旧製品、旧システムが一部に介在したときの全体セキュリティ低下

システムセキュリティ

- SaaS、アウトソーシング、データセンターなど、セキュリティ管理場所、要件が変化
- 新しい製品・サービスなどのソフト開発時に発生するバグ
- 新しく開発したソフトウエアで、セキュリティ脆弱性が枯れたことを検証する簡単な方式がない
- 統合化されたセキュリティ製品の開発、保守の複雑化から生じるバグ

状況仮説2に基づいた課題
（ユーザ）

課題

管理できないユーザ

- 高齢者、低年齢層へのIT普及により、リテラシー、セキュリティ意識の低下
- 犯罪組織の資金調達手段が先進ITで高度化、国際化
- 出会い系、自殺系、殺人請負サイトで発生する犯罪の防止
- ソーシャルエンジニアリングへの知識、意識が低い

状況仮説3に基づいた課題
（企業・個人の周辺環境）

課題

新しい使い方

- 持ち運び可能なデバイス(携帯電話、ICカード、RFIDなど)に対するセキュリティ
- ICカード、RFIDからの電磁波解析による秘密情報漏えい

新しいデバイス

- 情報家電のBOT化対策、情報家電へのパッチ配布の管理
- 情報家電などを遠隔保守する場合の保守チャネルの悪用対策
- 新型vs旧型、ベンダー間でのセキュリティ製品機能の互換性、管理一貫性の保障がない

新しいサービス

- 加速する企業統廃合、買収、外資化などによる製品・サービス継続性への不安

付録：課題リスト

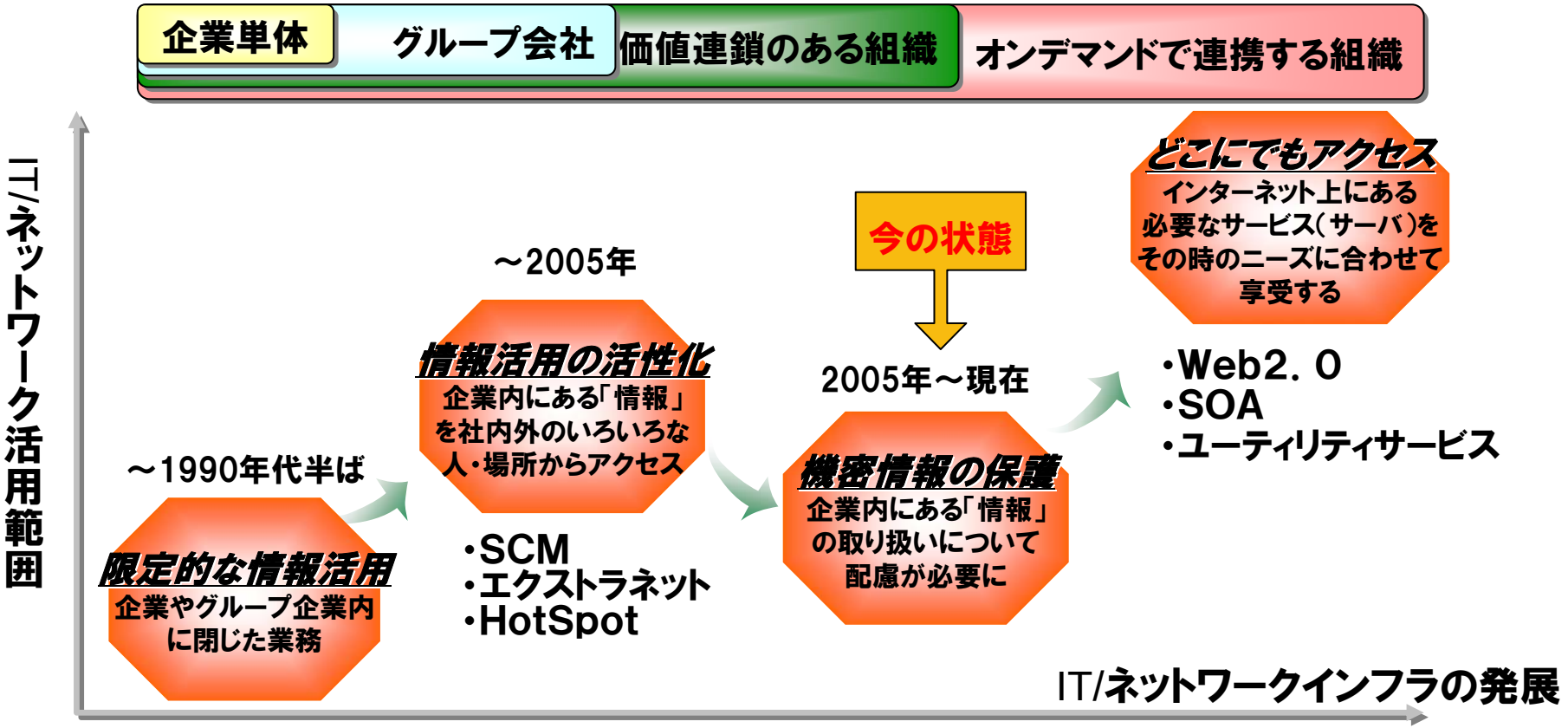
- 持ち運び可能なデバイス（携帯電話、ICカード、RFIDなど）に対するセキュリティ
- ICカード、RFIDからの電磁波解析による秘密情報漏えい
- 現PC同様の脅威群が無数の携帯で発生したときの管理
- セキュリティ管理が複雑になり管理上のミス多発に対する対策
- 管理対象の分散化、運用管理組織の縮小による出現する無管理空間への対策
- SaaS、アウトソーシング、DCなど、セキュリティ管理場所、要件が変化
- 新しい製品・サービスなどのソフト開発時に発生するバグ
- 新しいソフトウエアをセキュリティ脆弱性が枯れたことを検証する方式
- 統合化されたセキュリティ製品の開発、保守の複雑化から生じるバグ
- 高齢者、低年齢層へのIT普及により、リテラシー、セキュリティ意識の低下
- 犯罪組織の資金調達手段が先進ITで高度化、国際化
- 出会い系、自殺系、殺人請負サイトで発生する犯罪の防止
- 情報家電のBOT化対策、情報家電へのパッチ配布の管理
- 遠隔保守する場合の保守チャネルの悪用対策
- 旧式製品、システムが介在したときのセキュリティ低下
- 加速する企業統廃合、買収、外資化などによる製品・サービス継続性の不安
- 新型vs旧型、ベンダー間でのセキュリティ製品機能の互換性、管理一貫性

５年先を考えた企業での対策

インフラの進化に見るビジネス環境の変化

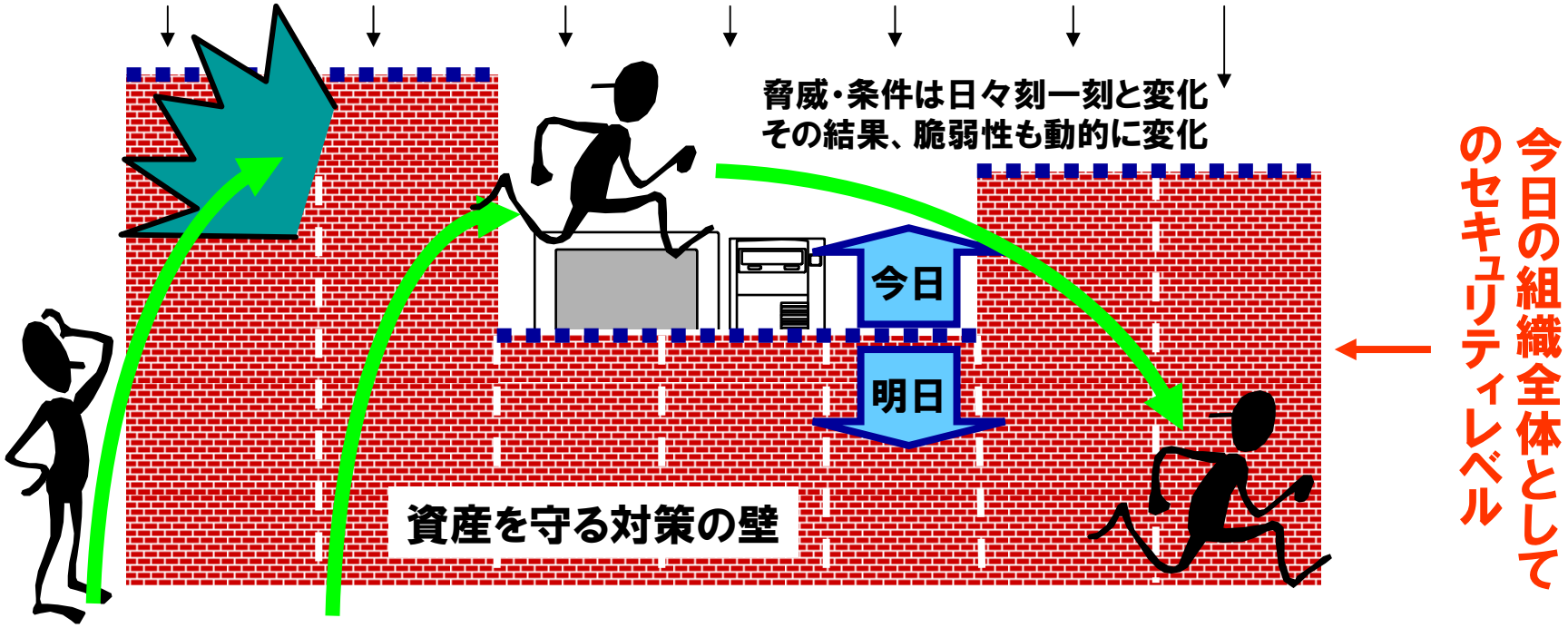
新しい情報サービスの利用で、
新しいビジネス機会の創出が可能

新しい環境に合った<u>セキュリティ対策</u>が重要に！



課題１：セキュリティの特性

個別対策の集まりでは脆弱性の変化に弱い



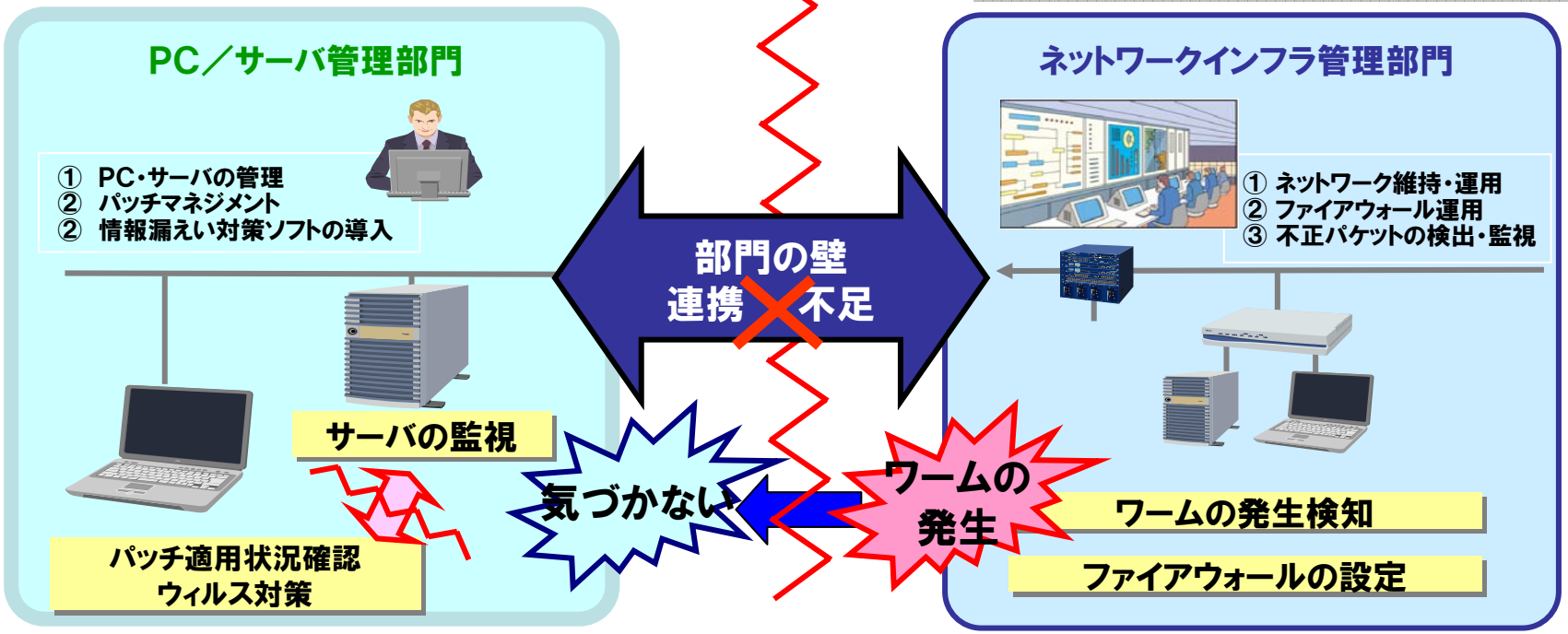
意識レベル低い部門・ユーザーの運用が内部犯行（意識的、無意識に関わらず）の温床に
外部からの脅威によって仕掛けられた“ウラ口（バックドア）”が外部犯行の温床に

課題２：セキュリティマネジメントの不整合

不整合１：　各ポイントで運用者が違う
不整合２：各ポイントでの対策間に抜けが生じる

・部門間の調整
・被害の拡大を未然に防げない
・各部門で対策を強化しすぎて利便性が低下してしまう。

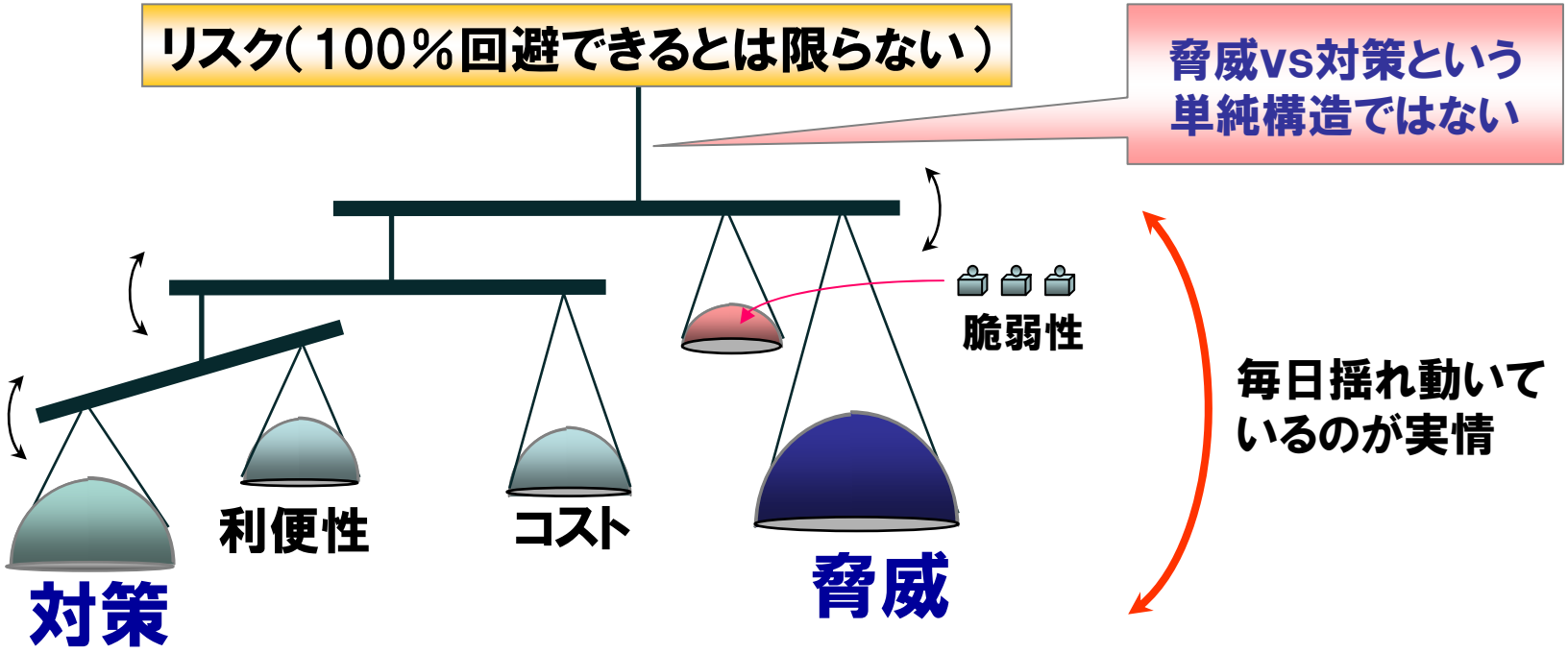
ITを上手く活用できていない！！
・運用・維持コスト増大
・人海戦術対応の限界



課題3：環境変化により難しいセキュリティ投資判断

インシデントの発生にパッチワークをするのではなく、「リスク全体」を理解し、継続的、全体的な対策を考えることが重要！

リスクに対する考え方とは



リスク分析：

1. 資産の洗い出しと資産価値（被害金額）の評価
2. 脅威の洗い出しと発生頻度の評価
3. リスク評価（被害金額×発生頻度）
   - 仮定をおいて金額の算出を行う
4. リスク低減目標の設定（緊急度、コストなどを加味）
5. 目標に応じた対策の洗い出しと実施

動的に変化

残留リスクへの対策

・脅威の回避、移転、または保有

脅威、対策、対策効果、効果の無効化、次の対策

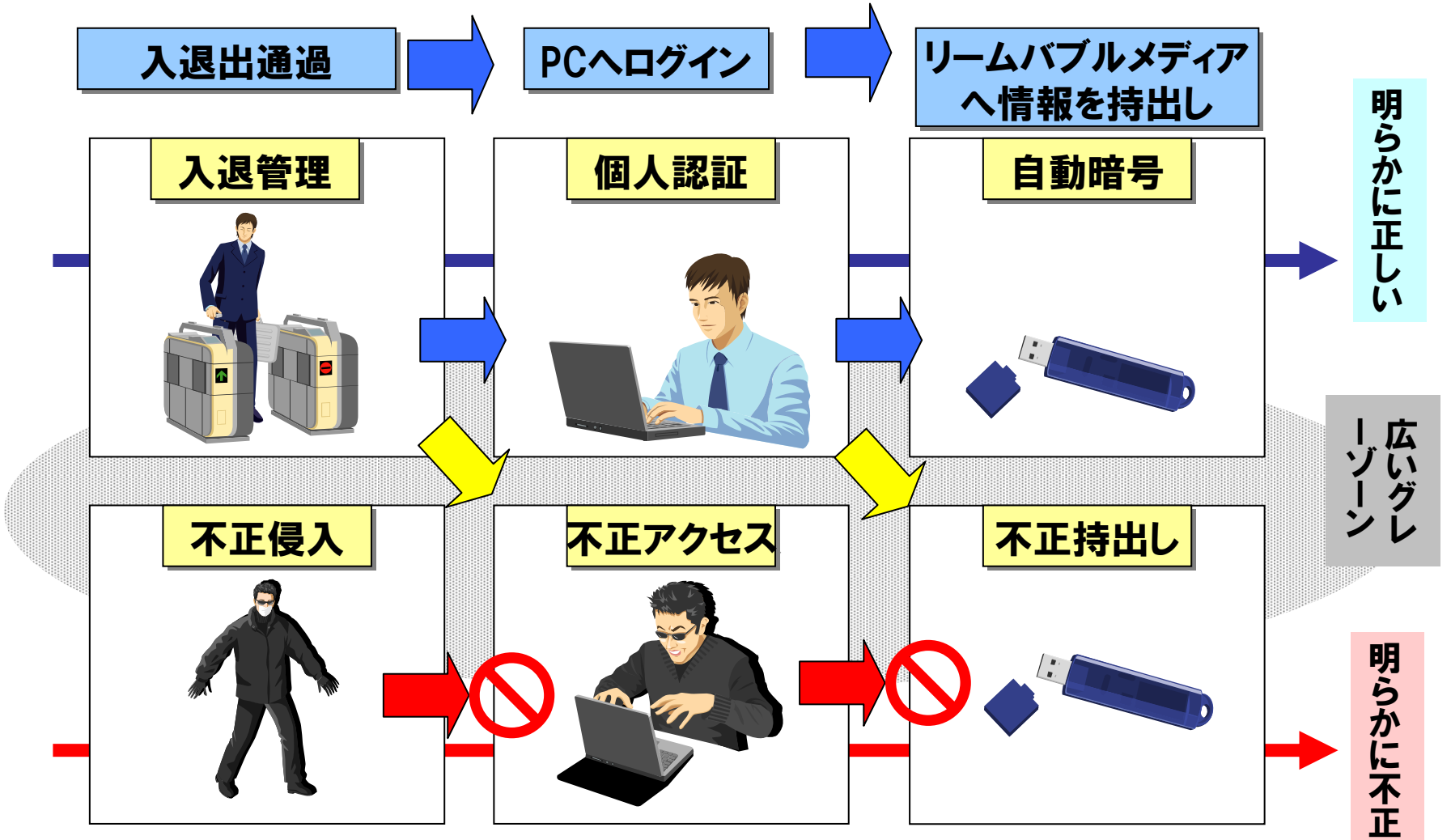
脅威の存在場所	脅威の内容	脅威に対してとられている対策内容	対策が効果を発揮する条件	対策が無効にされてしまう場合	対策の無効化を補う方法
PC	ワーム・ウィルスによる情報の拡散	ゲート上でワーム・ウィルスを除去	データが暗号化されていない	シグネチャの無い新種ワーム・ウィルス	①PCの隔離 ②サーバへのアクセス制御
PC	汚染されたPCの持ち込み	PC検疫システムで汚染状況を把握	PCに検疫エージェントを導入	検疫エージェントがとめられる	③ゲート上でワーム・ウィルスを除去 ④PCの隔離
PC、ファイル	ネットワーク経由でファイルを持ち出し	リモートデスクトップなどのプログラム起動禁止	共有情報のアクセス権強化	プログラム名を変更して起動	ファイル暗号化とアクセス権限管理
PC、ファイル	リムーバブルメディアでファイルを持ち出し	外部記憶デバイスへの書き込みは自動的に暗号化	必ずユーザ認証、PCを利用するのは一人	認証が省略される 認証済みのPCが悪用される	リムーバブルメディアの切り離し
PC、ファイル	メールにファイルを添付し不用意に送信	重要ファイルの常時暗号化	暗号鍵利用可能範囲での利用	編集作業などファイルを一次的に平文で保存	⑤メールサーバで平文ファイルをフィルタ ⑥PCの通信をロック
サーバ	不正ユーザによる操作	ICカードなど多要素認証の利用	個人に対する認証	カードの共有	認証条件、アクセス管理強化
ネットワーク	WAN上でのデータ盗聴	SSL、IPSECで通信を暗号化	VPNが作れる環境	平文に戻す装置より先の通信管理	ファイルの暗号化

＊これらは一例、実環境では何百というリストが出てくる

変化に柔軟に対応する考え方が不可欠

「次の対策」が必要にされる例

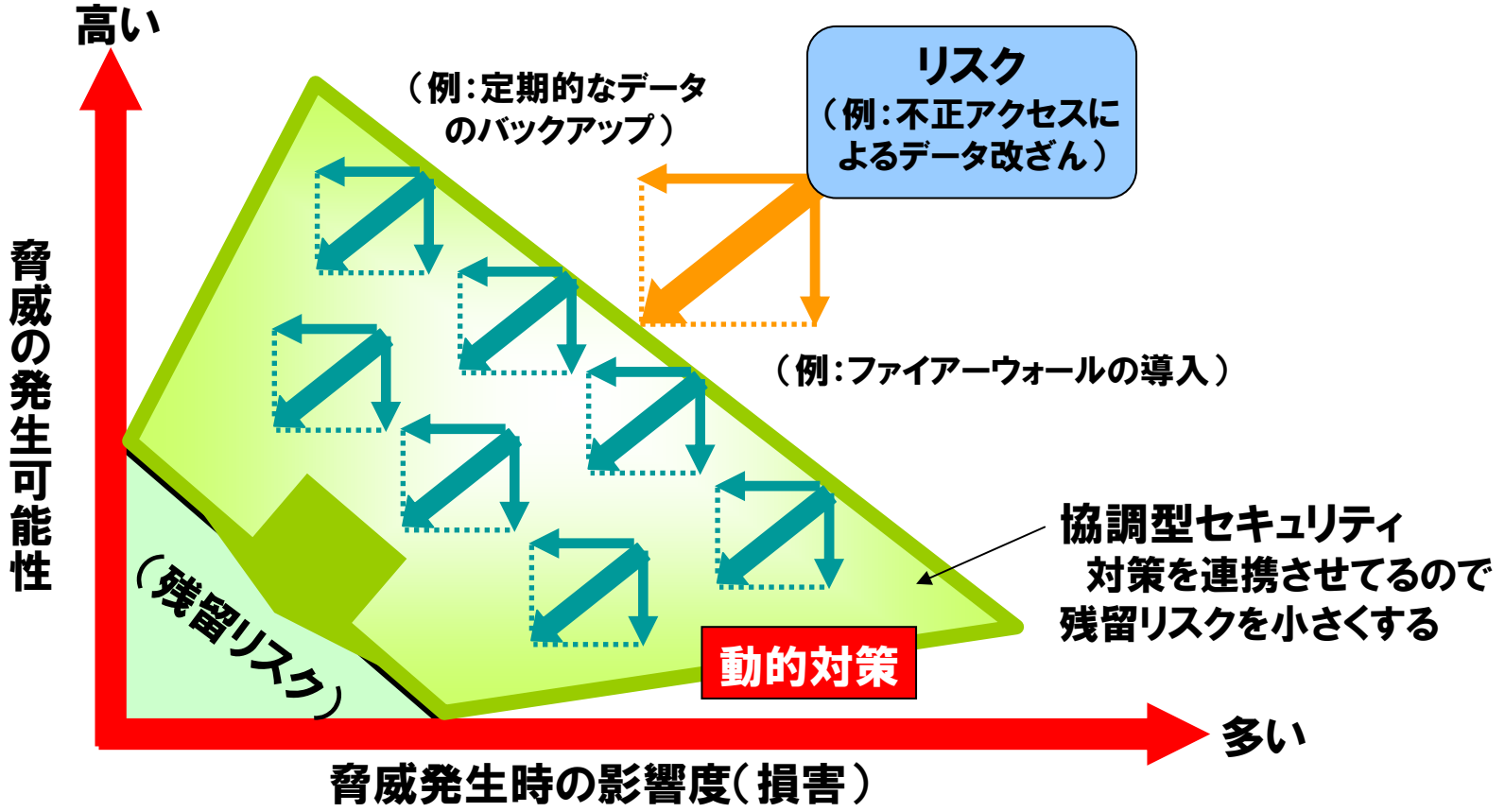
各対策では防げない事象は他の対策を組み合わせて対策を行う。
さらに各対策を連携することで、セキュリティレベルを向上させる。



リスク管理と協調型セキュリティ

協調型セキュリティの考え方

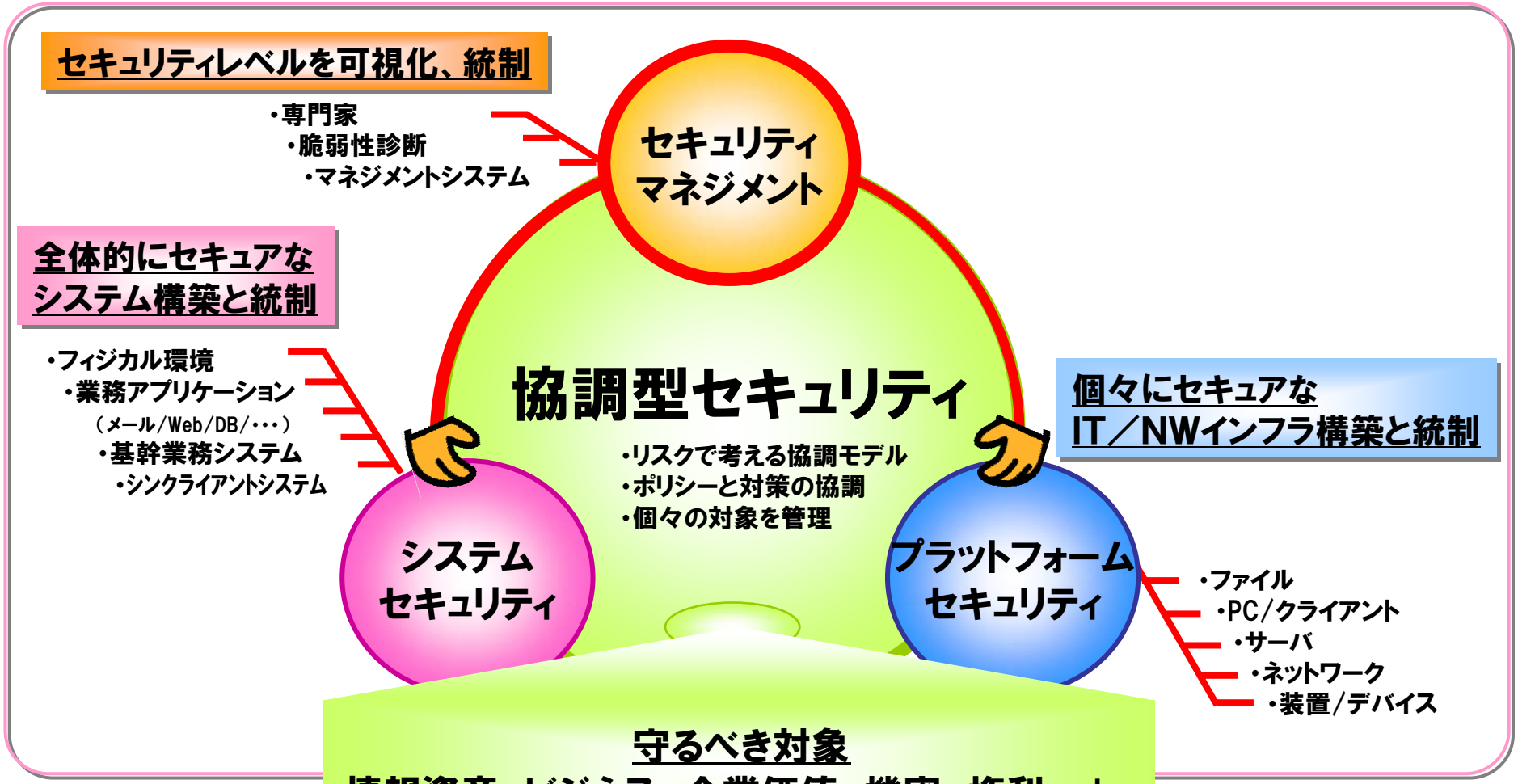
1. 個別対策効果の連携を取る
2. リスクモデルを拡張、動的な脅威、条件の変化に対応する
3. 環境変化で生じる対策の無効化を別の対策でカバーする



「リスク管理」を基本に、セキュリティ
マネジメントから、全体的視点で考える
セキュリティ「協調型セキュリティ」

セキュリティへの新しい考え方

セキュリティ対策間を連携させ、個々で生じる新たな脆弱性を、他で埋める「協調型セキュリティ」で組織的範囲でマネジメント



効果的にリスクを埋める階層構造

各レイヤーで得意な対策を組み合わせて高度なセキュリティ対策を実現する。
さらに対策を連携・協調させることで、利便性を維持した対策を実現する。

「協調型セキュリティ」動作例

協調エンジンの動作例(１)

ポリシー／モデル

1 **サーバに登録されている**RemoteUser**は、ネットワーク越しにログオンできる**
2 Level**が**confidential**なサーバへのネットワークアクセスは最小にする**
3 Level**が**confidential**なサーバへのネットワークアクセス中は、文書のクライアントへの保存を禁止する。また、USBメモリの利用は禁止する。**
4 3.**以外の場合はファイル保存可能で、**USB**メモリを利用可能。**

ポリシー1,2**を満たす協調動作を実現**

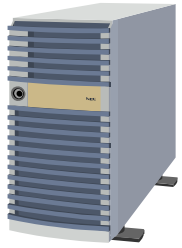
③ポリシー1**を評価するために、個人情報管理サーバの** RemoteUsers**をチェック**

協調管理サーバ

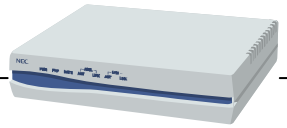
②pc1**上のエージェントが協調管理サーバにユーザのログオンを通知**

④ポリシー1**とポリシー**2**を満たすように、ファイアウォールの設定を変更**

①A**さんがクライアント** pc1**にログオン**



個人情報管理サーバ



ファイアウォール

pc1

Level = ‘confidential’
IPAddr=10.56.2.1
RemoteUsers = {A**さん**, B**さん**}
LogonUsers = {}

permit 10.56.1.122 10.56.2.1
deny any 10.56.2.1

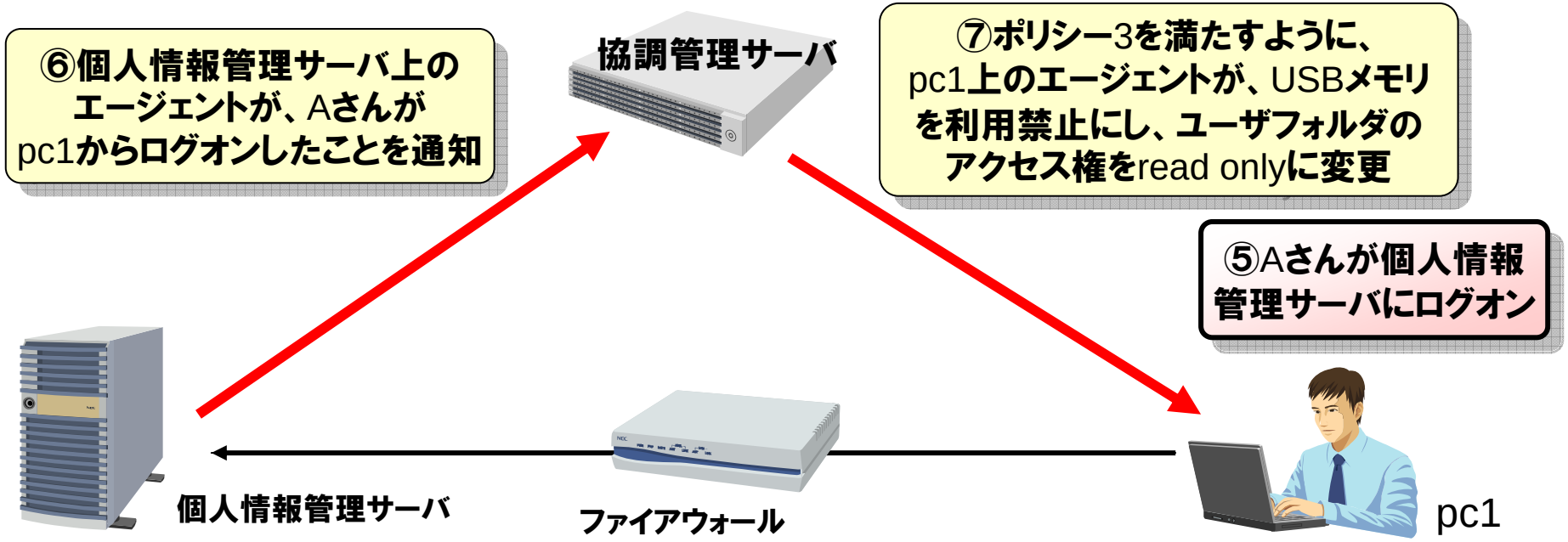
IPAddr=*10.56.1.122*
LogonUser=‘A**さん**’
USBMemEnabled=*true*
HomePermission = *full*

協調エンジンの動作例(２)

ポリシー／モデル

1 **サーバに登録されている**RemoteUser**は、ネットワーク越しにログオンできる**
2 Level**が**confidential**なサーバへのネットワークアクセスは最小にする**
3 Level**が**confidential**なサーバへのネットワークアクセス中は、文書のクライアントへの保存を禁止する。また、USBメモリの利用は禁止する。**
4 3.**以外の場合はファイル保存可能で、**USB**メモリを利用可能。**

ポリシー3,4**を満たす協調動作を実現**



Level = ‘confidential’
IPAddr=10.56.2.1
RemoteUsers = {A**さん**, B**さん**}
LogonUsers = {A**さん**@pc1}

permit 10.56.1.122 10.56.2.1
deny any 10.56.2.1

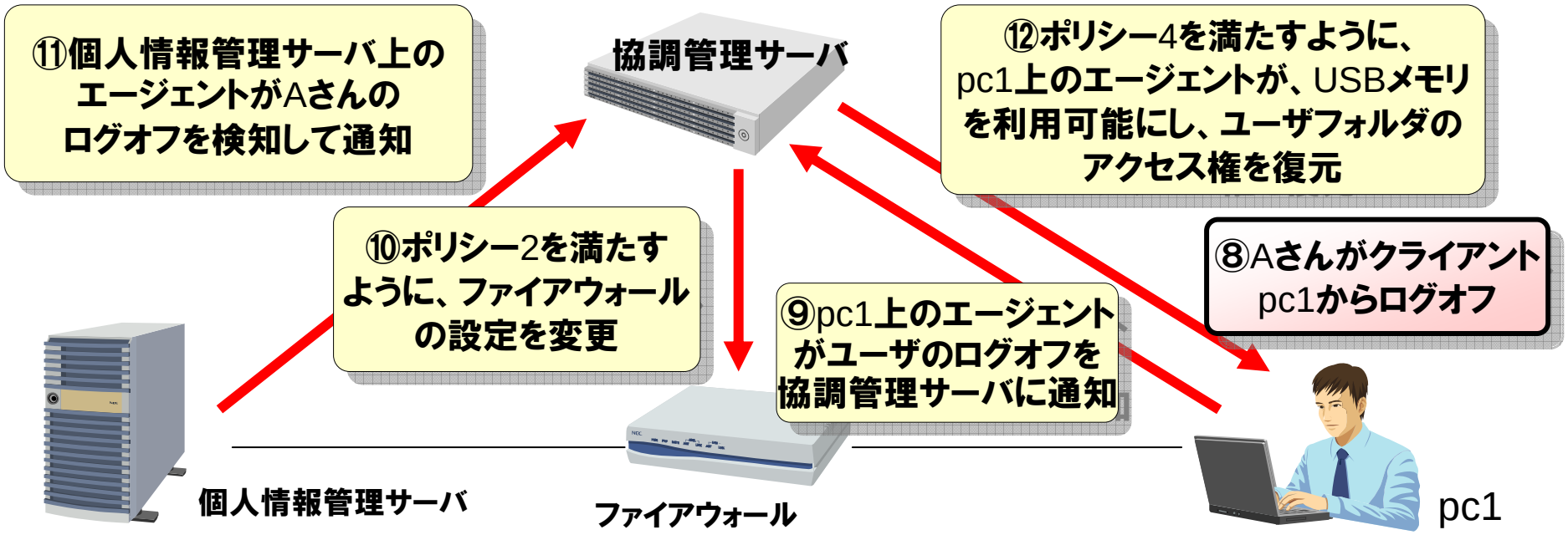
IPAddr=*10.56.1.122*
LogonUser=‘A**さん**’
USBMemEnabled=*false*
HomePermission = *readonly*

協調エンジンの動作例(３)

ポリシー2,4を満たす
協調動作を実現

ポリシー／モデル

1 **サーバに登録されている**RemoteUser**は、ネットワーク越しにログオンできる**
2 Level**が**confidential**なサーバへのネットワークアクセスは最小にする**
3 Level**が**confidential**なサーバへのネットワークアクセス中は、文書のクライアントへの保存を禁止する。また、USBメモリの利用は禁止する。**
4 3.**以外の場合はファイル保存可能で、**USB**メモリを利用可能。**



Level = ‘confidential’
IPAddr=10.56.2.1
RemoteUsers = {A**さん**, B**さん**}
LogonUsers = {}

deny any 10.56.2.1

IPAddr=*10.56.1.122*
LogonUser=‘’
USBMemEnabled=*false*
HomePermission = *full*

おわりに

5年先の対策に向けた提言

- 企業内でとられるセキュリティ対策と管理は、この数年でかなり成熟する。この成熟化ノウハウを、NGN、情報家電、モバイルに対するセキュリティ管理に生かせる。
- 業務、サービスを、エンド・ツー・エンドで保障するには、企業内と企業外（NGN上など）のセキュリティ方式で互換性があり、通信透過性を保障する必要がある。
- 技術では解けない問題、解けても製品が提供されないことがある。こういう領域には政策で取り組む必要がある。
  - 非企業ユーザのリテラシー、モラル
  - 犯罪者に動機付けを促すサービス
  - 対策を提供してもビジネスになりにくい領域
  - 技術がまだ見えない（脆弱性が未知）領域