FUJITSU THE POSSIBILITIES ARE INFINITE

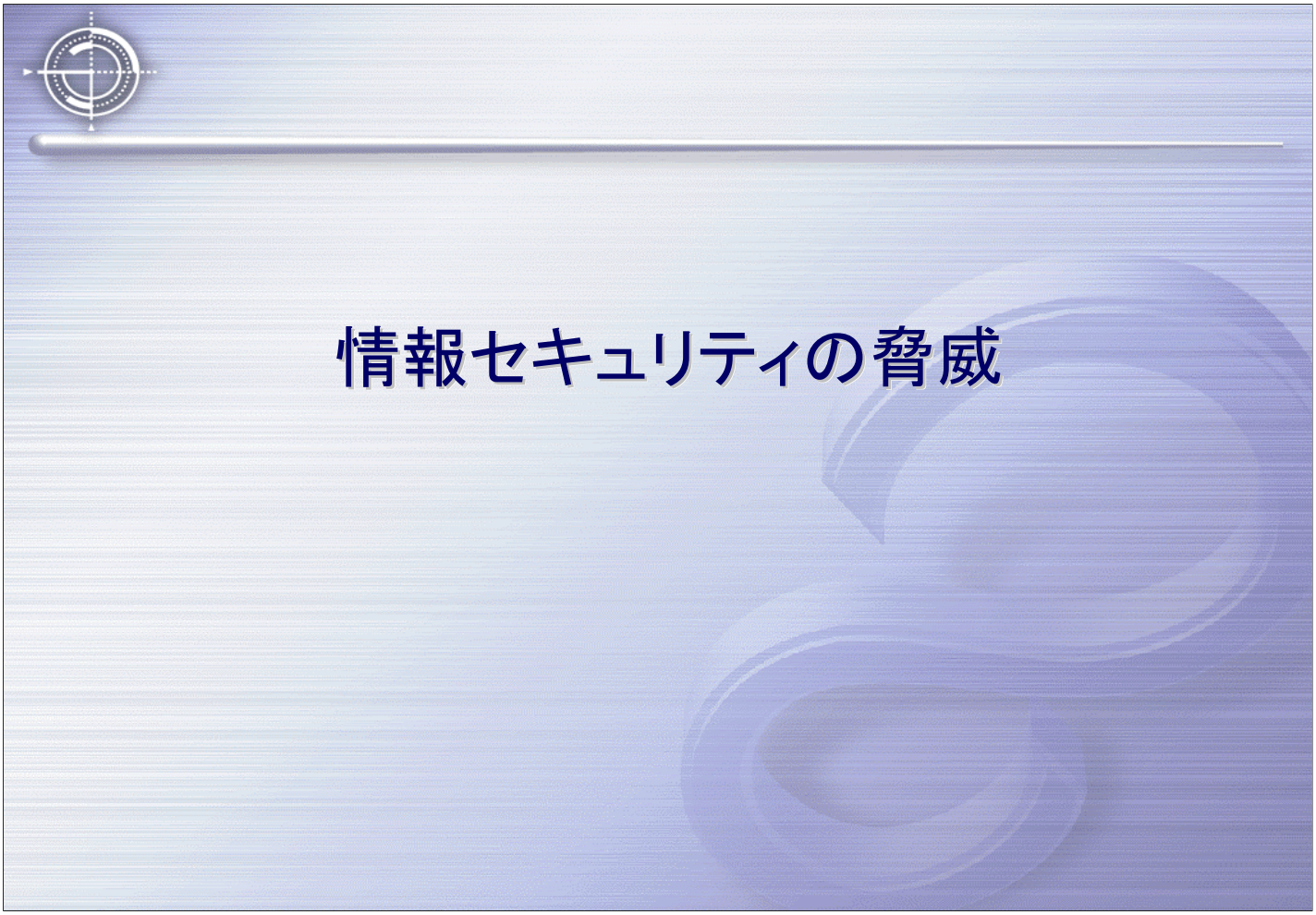
不正アクセスの現状と富士通の取組み

～ よりセキュアなシステム構築のために ～

平成13年 8月

富士通株式会社

紛争の話があったが、不正アクセスの被害を発生させないことが最も大切。
世の中の状況や対策について。



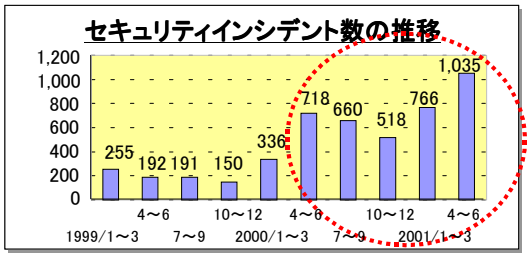
不正アクセスの動向について。

ネットワークコンピューティングの脅威

■急増する不正アタック

JPCERT(ｺﾝﾋﾟｭｰﾀ緊急対応ｾﾝﾀｰ)への届出状況

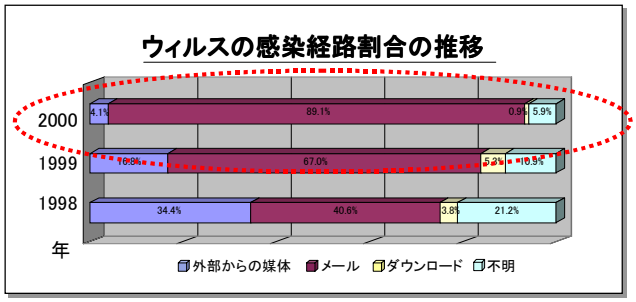
1996年10月～ 2001年6月 ： 6,267 件

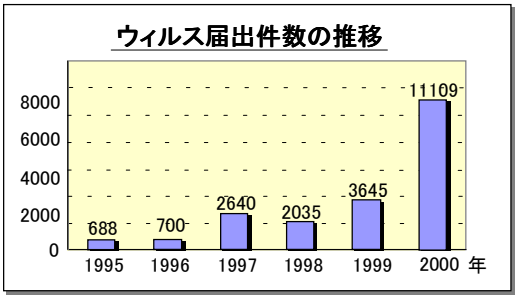


■ウィルス感染の約90%がメールから

IPA (情報処理振興事業協会) への2001年1月～ 6月の報告状況

被害届出件数： 9,569 件



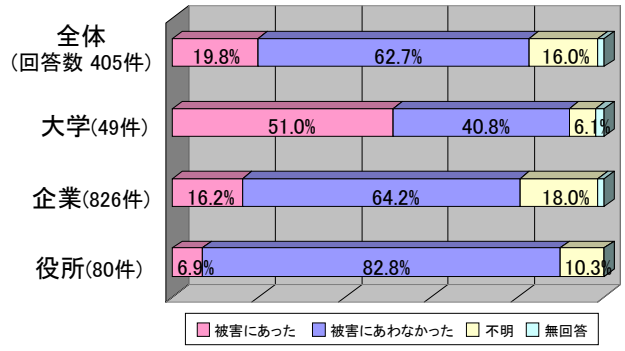


マスコミではあまりさわがれなくなったが、不正アクセスやウィルスのインシデントは非常に増えている。

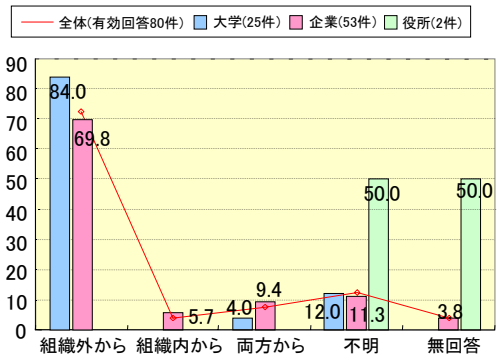
<参考>不正アクセス対策に関するアンケート報告書

警察庁ホームページ http://www.npa.go.jp/police_j.htm

過去1年間の不正アクセス等被害の有無



不正アクセスの発信源



調査期間：2000年10月～12月
調査対象：一部上場企業及び店頭登録企業、大学、役所を無作為抽出

**過去1年間で、ユーザ全体の約20%が不正アクセスの被害。
特に、大学の被害率は51%と突出。**

警察庁から公表された。
大学の被害が大きい（出入り自由）。

セキュリティの一般的な傾向(アタックテスト結果より)

1. Microsoft IIS 4.0/5.0 Escaped Characters Vulnerability 等 **88%**

Microsoft IISを使ったシステムに対する最新のパッチの未適用や、標準でインストールされる脆弱性を持ったサンプルプログラムの存在の指摘

2. “Smurf” Attack (ICMP Amplifier) **63%**

ブロードキャストアドレスへのICMP Echo Requestに対して装置が応答してしまう事の指摘
(このことを利用したDoS攻撃“Smurf”の被害に遭う可能性がある)

3. Multiple Vendor BIND iquery Buffer Overflow Vulnerability 等 **55%**

古いBINDプログラムの使用に関する危険性の指摘

4. Mail Relay **17%**

メールシステムが第三者転送をする設定になっていることの指摘
(第三者転送を可能にしているとスパムメールの踏み台にされる危険性がある)

5. “sendmail”ETRN Denial of Service **17%**

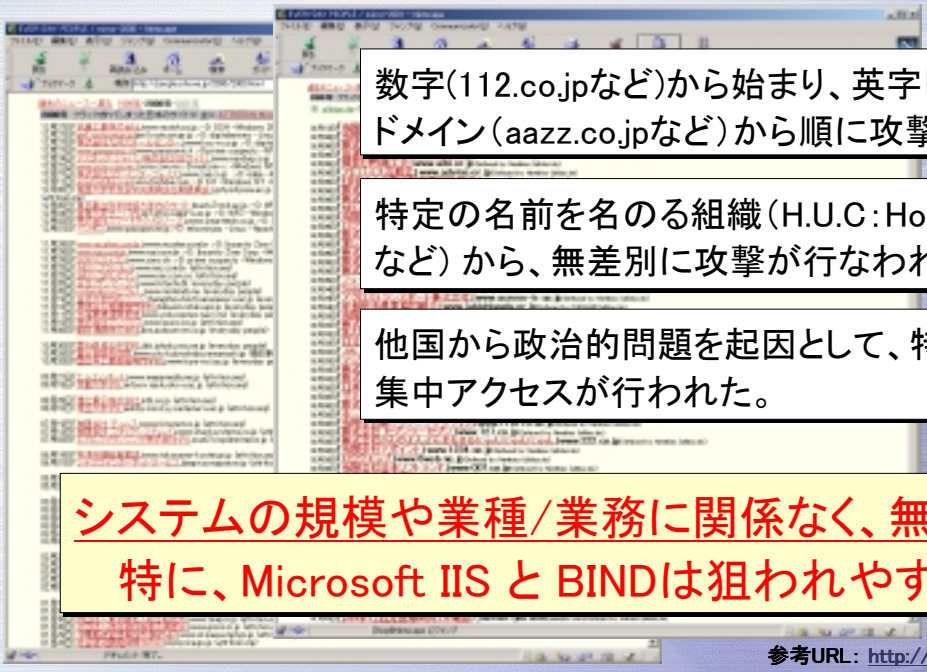
SendmailのETRNcommandに含まれる脆弱性の指摘

調査対象:70社

SS研／LS研のお客様を対象に後述のアタックサービスエクスプレスを使って分析した結果。(ワースト5)

jpドメインに対するアタックの増加

2001/1末より、jpドメイン(*.co.jpなど)に対してのホームページ改ざんが急増中



数字(112.co.jpなど)から始まり、英字「a」から始まるドメイン(aazz.co.jpなど)から順に攻撃が行なわれている。

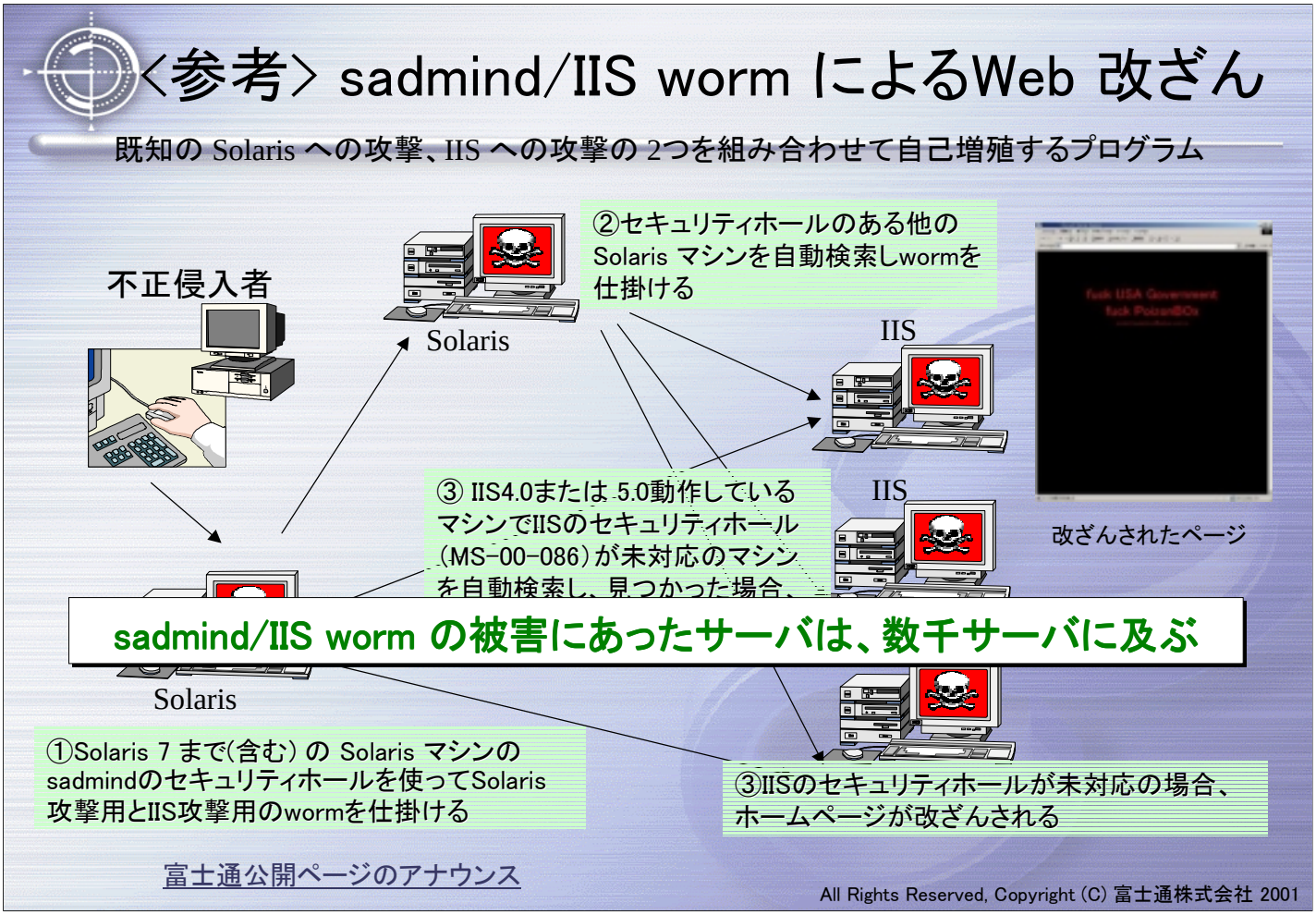
特定の名前を名のる組織(H.U.C:Honker Union of Chinaなど) から、無差別に攻撃が行なわれている。

他国から政治的問題を起因として、特定サイトへの集中アクセスが行われた。

システムの規模や業種/業務に関係なく、無差別に攻撃。
特に、Microsoft IIS と BINDは狙われやすく要注意！

参考URL: http://people.site.ne.jp/2001/2001.html

不正アクセスの傾向が今年から大きく変化している。
著名な企業から無差別にセキュリティホールをねらわれる。
セキュリティパッチの適用が非常に大切。



多量のサーバがクラックされた。
SUNの有名なセキュリティホールをついて侵入。

不正アクセスの増加要因

◆アンダーグラウンドでの情報交換
- ハッカー/クラッカーの組織化，ハッキング情報等の共有，クラッキングツールの流布

◆雑誌や本での技術情報の提供
- プロでない学生や一般人による行為

◆無防備なユーザの急激な増加（ブロードバンドの普及）

◆セキュリティホール(プログラムバグ等)への対応遅れ
- バッファオーバーフロー等のアタック，メール不正中継，ウィルス

◆高度なハッキングツール・手法等の出現
- ポートスキャン / パスワードクラッキングツール / ネットワーク盗聴、等

◆新しいセキュリティ情報への対応が困難
- 複雑なシステム構成　人材、24時間/365日監視等の運用体制

無防備なユーザが増えた。→ブロードバンドで更に加速する。

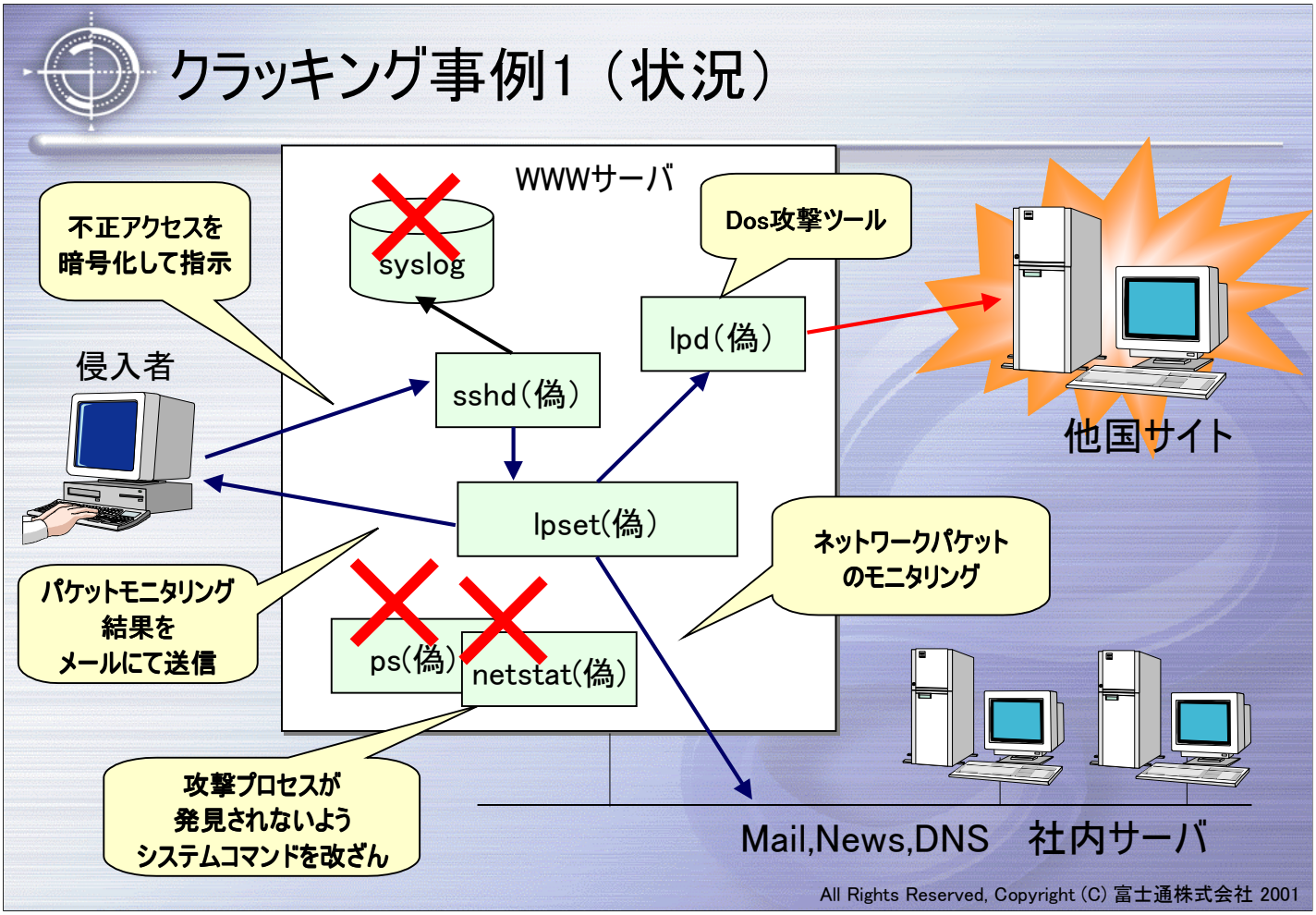
クラッキング事例1（事件経緯）

～ 被害者のつもりが自分も加害者に !! ～

- 一般利用者から、接続できない、などのクレームが来て
  回線業者による調査を依頼するが、自然復旧
- その後、何度も同様の現象が起こるが、自然復旧
- 複数サーバに侵入された形跡発見
  ログの欠落が多い(空白の期間がある)
  リブートの形跡がある

警察に通報/支援の依頼を決定
サーバファイルを詳細に調査することを検討

最初は、障害と思っていた。
調査を進めるうちに深刻な問題ということがわかった。



実は、DoS攻撃プログラムが仕掛けられ、サーバの負荷が上がっていた。

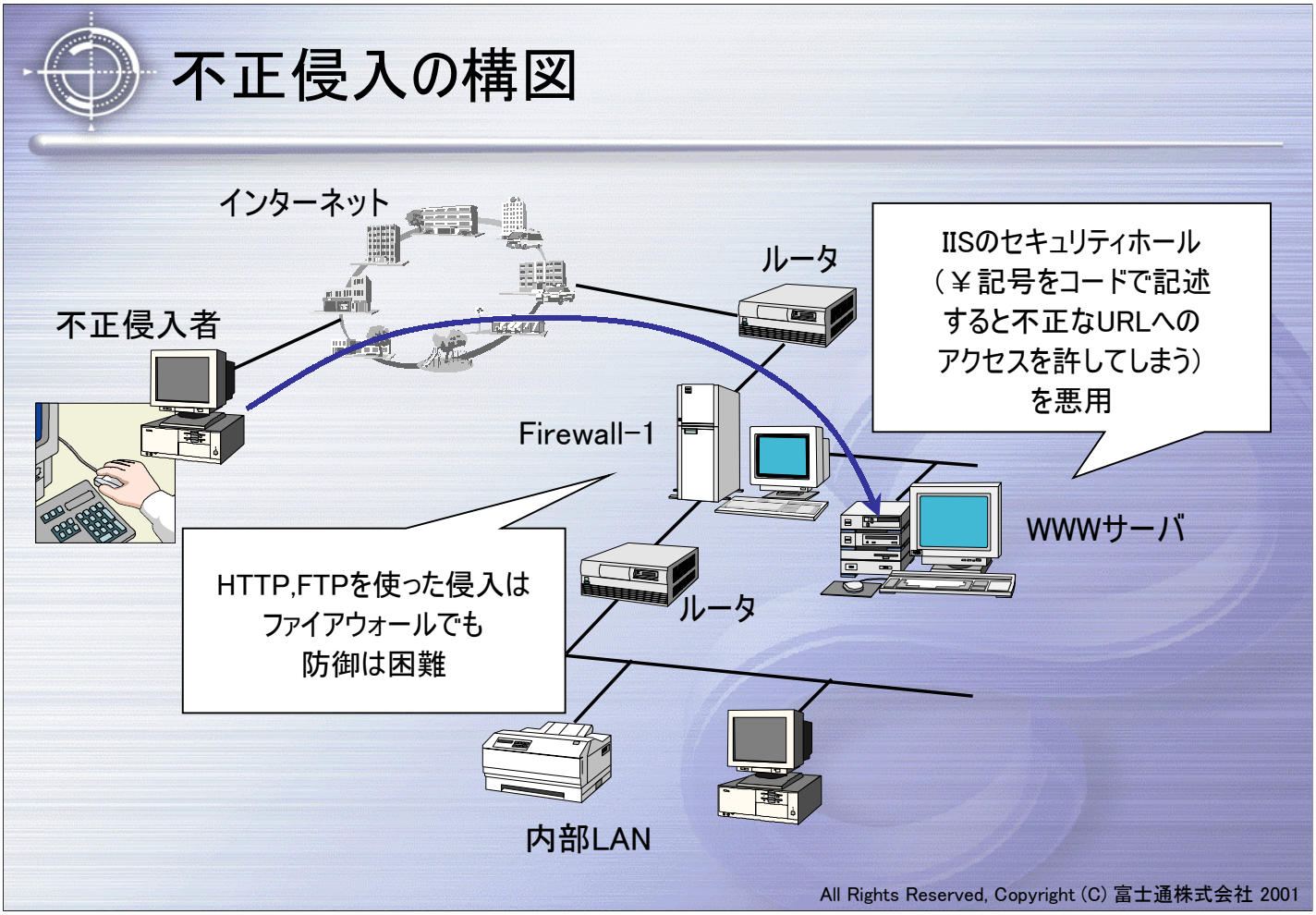
クラッキング事例2（事件経緯）

～ ファイアウォールを過信してはいけない !! ～

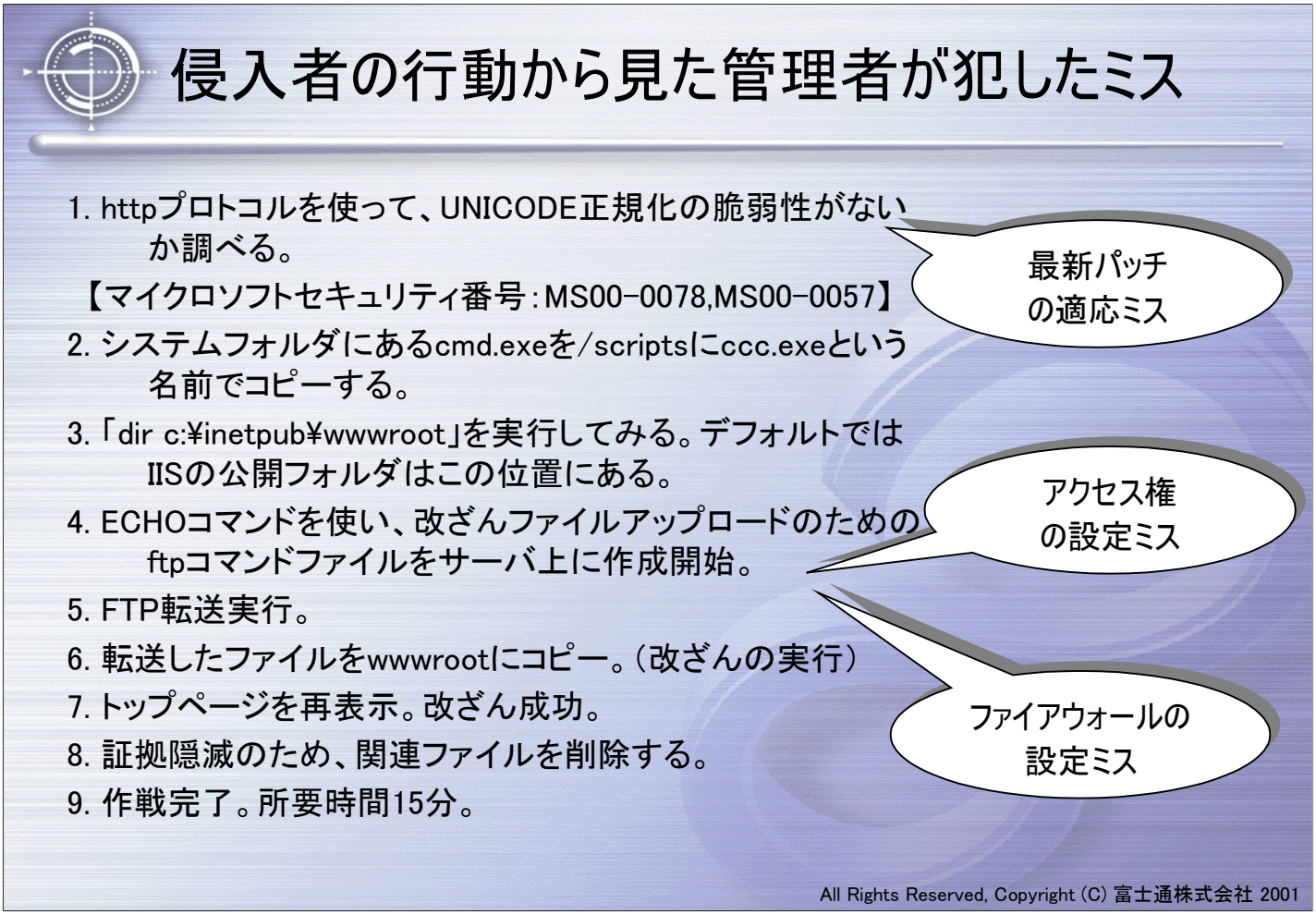
- 朝、ホームページが何者かに書き換えられているのを従業員が発見
- 書き換えられていた部分はホームページのトップページ
- 日頃から、ファイアウォールをレベルアップするなど、対策を講じてきただけに、関係者はショック

警察に通報/支援の依頼を決定
サーバファイルを詳細に調査することを検討

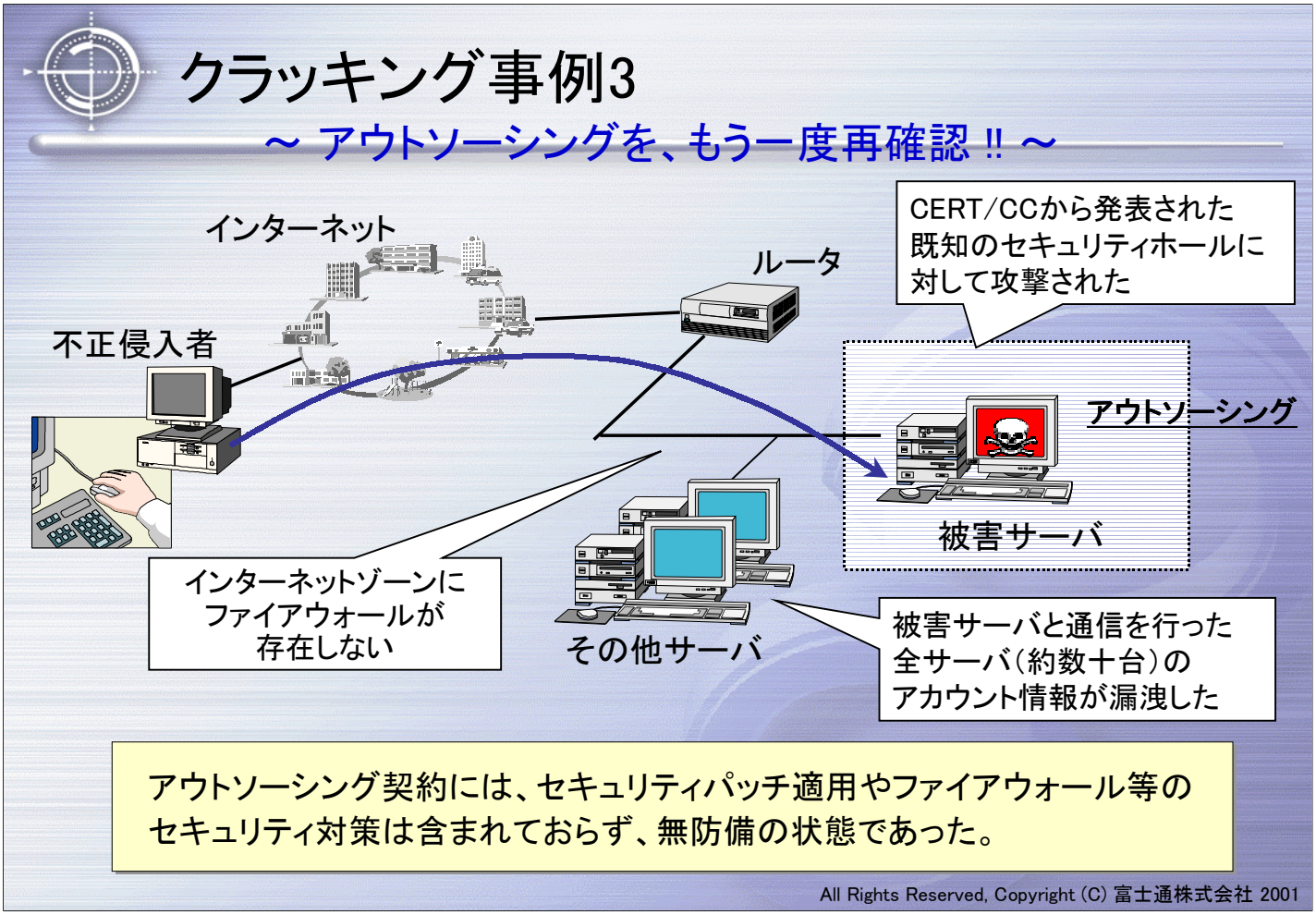
ファイアウォールを導入して、数ヶ月後にクラック。



IISのセキュリティホール。
セキュリティホールが公表されてからすぐにやられた（約2カ月）。



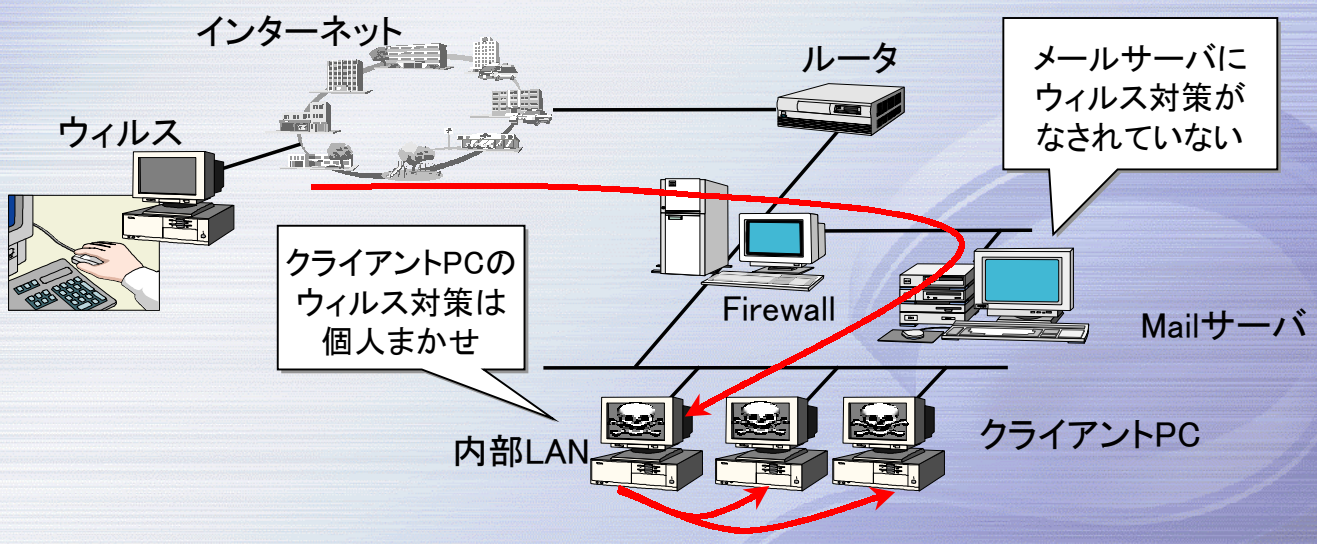
原因を分析すると3つのミスを侵していた。
①バッチ適用漏れ
②アクセス権を適切にしていなかった
③F/Wで外に見せてはいけないサービスを見せていた



アウトソーシングされた部分に落とし穴（F/Wなし）があった。
アウトソーシングされた部分の対応や責任分担を明確にしておくこと。

ウィルス被害事例

～ たった一通のウィルスメールで業務がストップ !! ～



メール環境の復旧のため、メール運用が1週間停止。

ウィルス駆除のため、人海戦術により全PC（数千台）に対して
ウィルスチェックソフトのインストールとチェックを実施。

クライアントのウィルス対策状況がきちんと管理されていなかったため、ウィルス対策がとれず数千台の全クライアントを再インストール。システムが1週間止まった。

事例に見るセキュリティのポイント

- インターネットゾーンには、ファイアウォールを必ず設置すること
- CERT/CCなどの最新のセキュリティ情報をチェックすること
- サーバを乗っ取られた場合、DoS攻撃やウィルスの加害者となり訴訟問題に発展する可能性もある
- アウトソーシングしているサーバの運用責任を再確認すること
- ウィルスを甘く見るな
  被害台数が多くなるため、対応・復旧に時間を要する

紹介した事例からポイントをまとめた。

企業や組織として対策する必要が大きくなっている。

e－Japan戦略

我が国は、すべての国民が情報通信技術（IT）を積極的に活用し、その恩恵を最大限に享受できる知識創発型社会の実現に向け、早急に革命的かつ現実的な対応を行わなければならない。市場原理に基づき民間が最大限に活力を発揮できる環境を整備し、５年以内に世界最先端のIT国家となることを目指す。

重点政策分野

①超高速ネットワークインフラ整備及び競争政策

競争及び市場原理の下、5年以内に超高速アクセスが可能な世界最高水準のインターネット網の整備（**少なくとも3000万世帯が高速網、1000万世帯が超高速網に常時接続可能**）

②電子商取引ルールと新たな環境整備

BtoB及びBtoC市場規模が**2003年に1998年の10倍の予測を大幅増**

③電子政府の実現

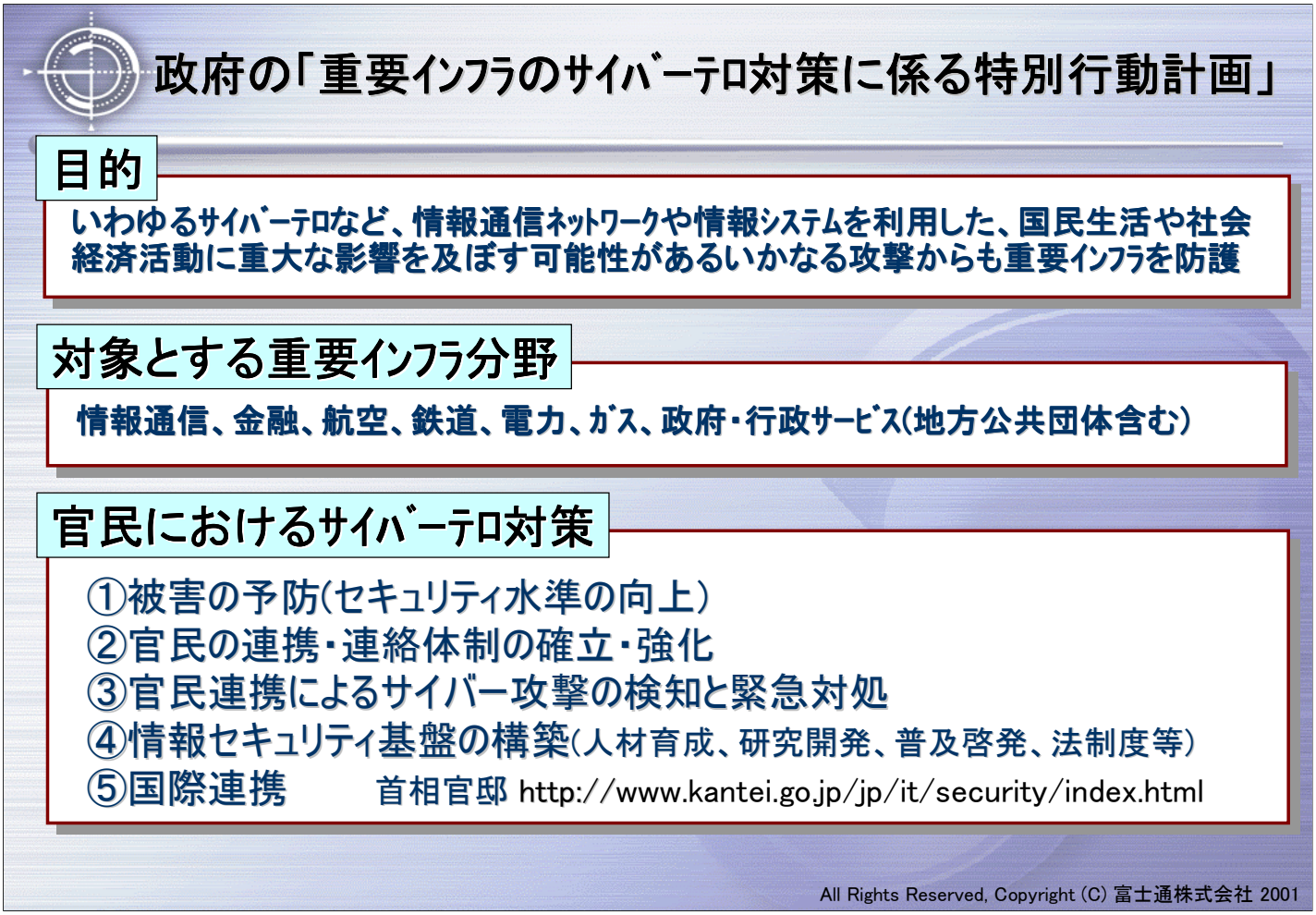
2003年度には**電子情報を紙情報と同等に扱う行政を実現**

④人材育成の強化

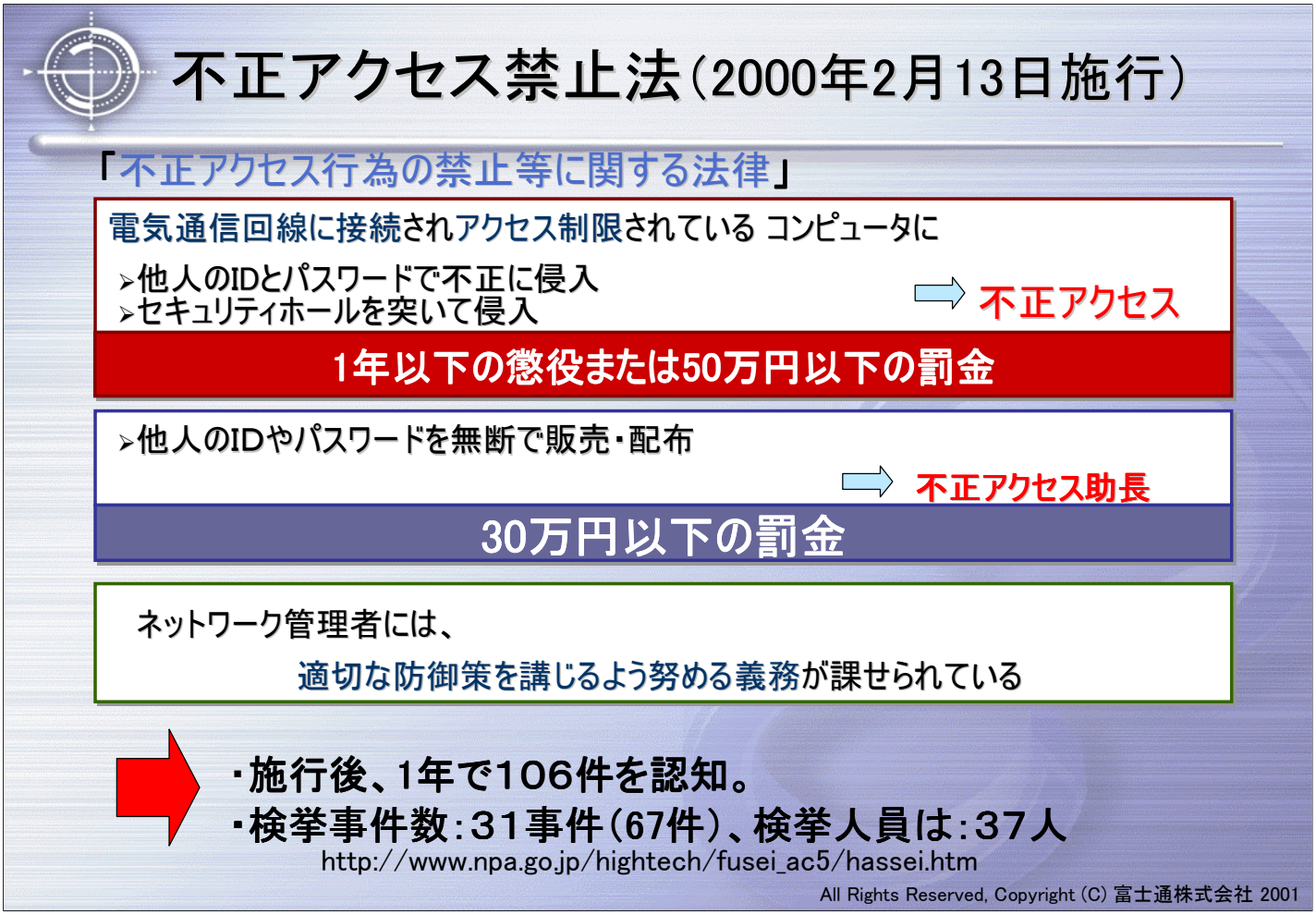
2005年のインターネット**個人普及率予測60%を大幅に上回る**

首相官邸 **http://www.kantei.go.jp/jp/it/network/dai3/jyuten/index.html**

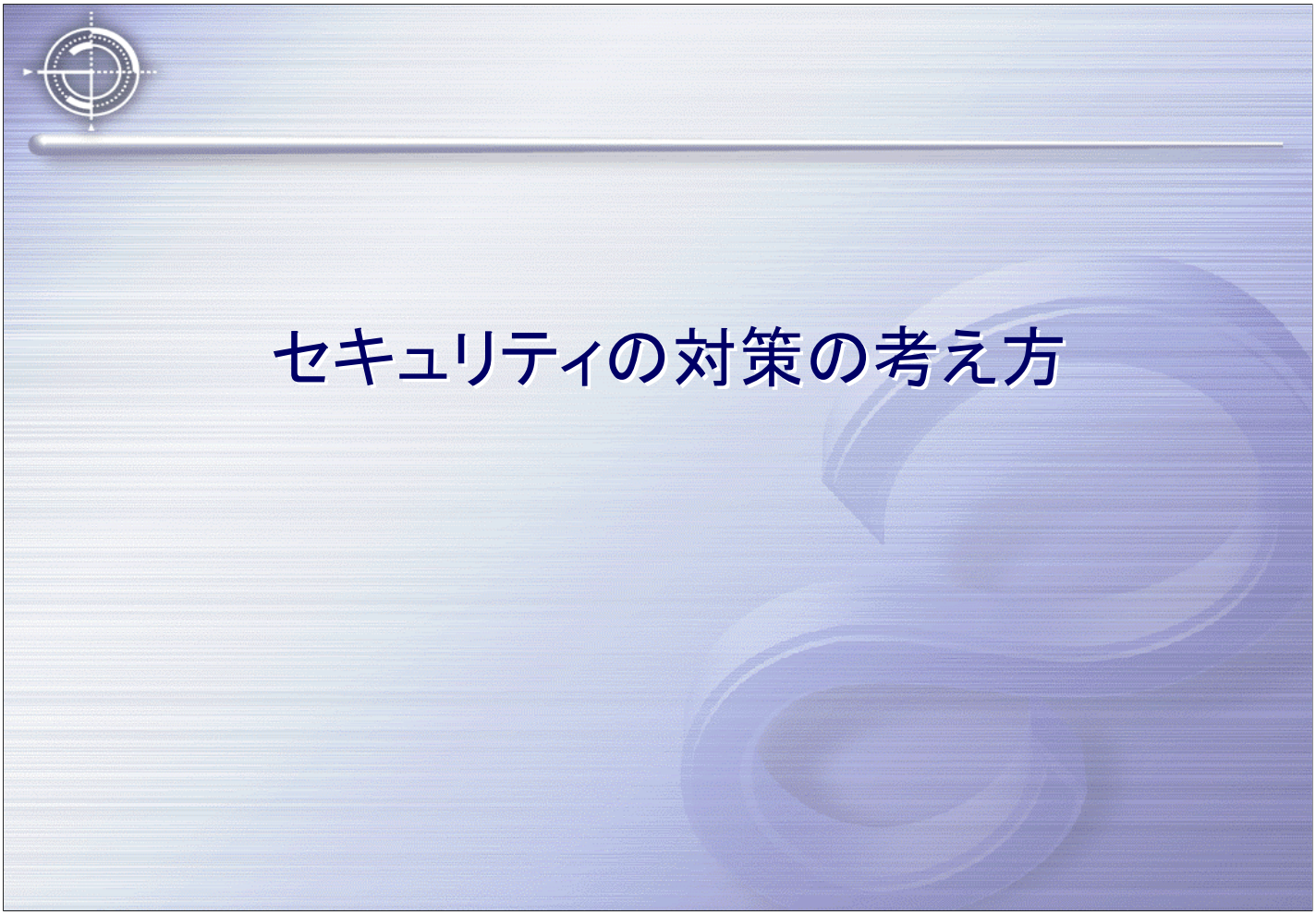
世の中が確実にインターネット化されていく。



国も率先して対策を促している。
電子政府等の実現とともにインフラ確保。

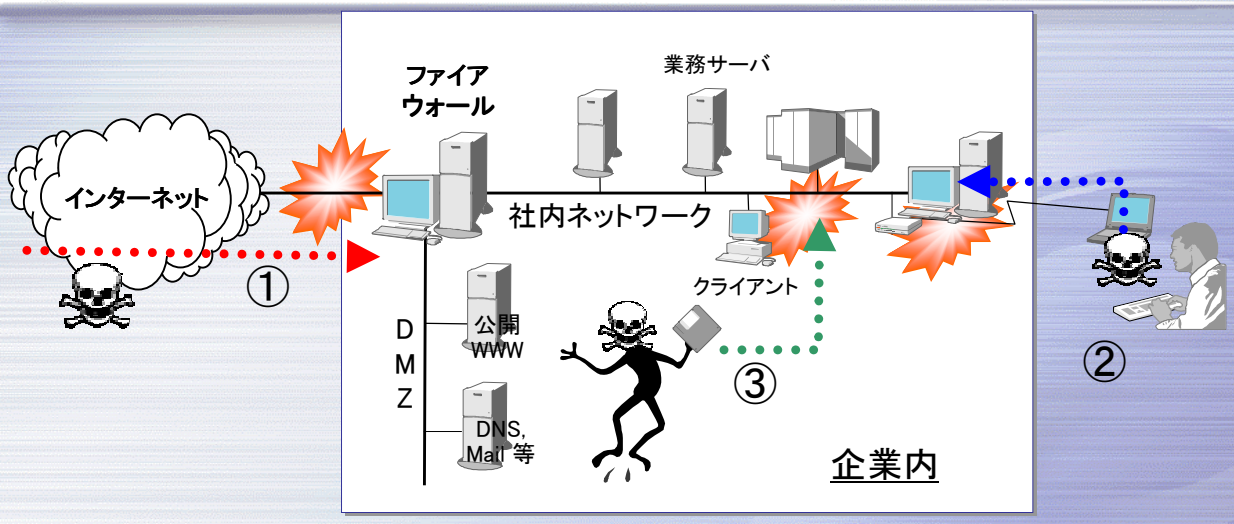


法的にも防御をしないといけない。
管理者は個人ではない。



世の中の動きや法的な観点からも、組織的にセキュリティ対策を行うことが重要だということがお分かりいただけたと思うが、具体的にとるべき対策について述べてみたい。

企業システムでの脅威の種類



①正面からの攻撃企業
②バックドアからの攻撃
} 外部からの攻撃への対策

③内部犯罪
} 内部の要員管理,機器管理,体制等

DMZ： Demilitarized Zone（非武装地帯、緩衝地帯）

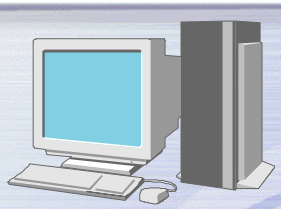
3つの切り口から対応すること。

①正面からの攻撃への対策

ファイアウォールの構築

＋

セキュア環境構築

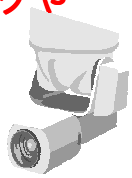


(1)堅牢なサーバ構築

- 不要なサービスの停止
- 不要なCGI(サンプルアプリ)削除
- デフォルト設定の見直し
- 最新ソフト/パッチの適用
- スパムメール対策

etc…

⇒攻撃のほとんどが、OS/アプリケーションのバグや設定ミスをついたもの。



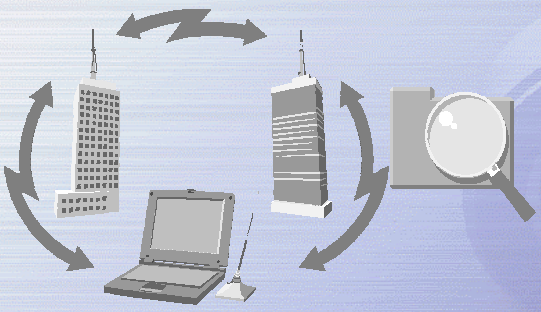
(2)セキュリティ監査の実施

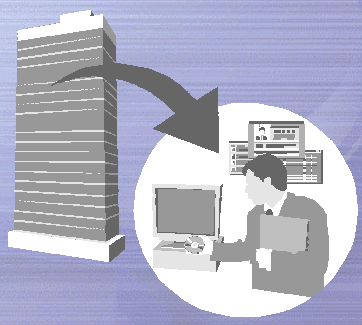
(3)不正アクセス監視の実施

1つ目は、F/Wとサーバ対策。

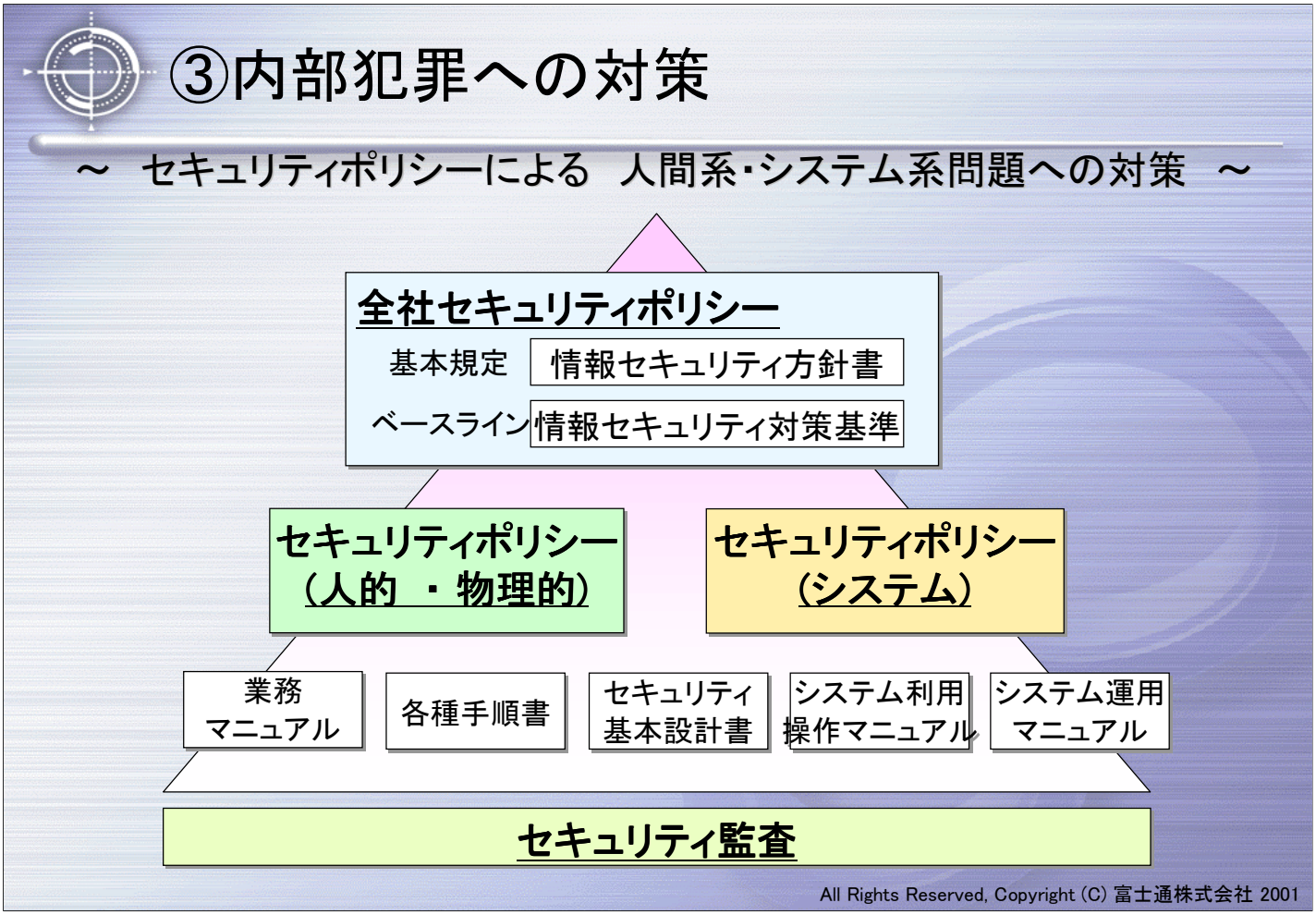
②バックドアからの攻撃対策

- 外部ネットワークとの接続口の局所化
- アクセス先,ファイアウォール/サーバ設定の確認
- 個人によるISP接続の禁止
- 従業員への周知徹底/教育
- ログの監視/監査　　等々





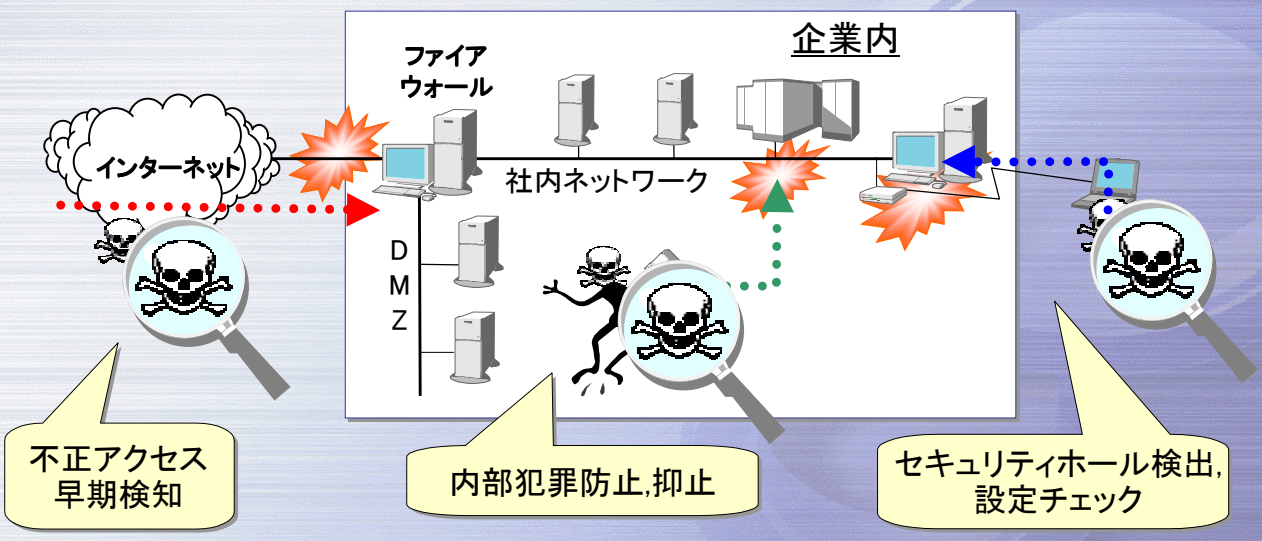
2つ目は、バックドア。基本的にはバックドアが発生しないよう管理や監視／監査をすること。



3つ目は、内部の不正に対する対策。
考え方やルールをドキュメント化し、人的な面・システムの面から対策を徹底すること。

セキュリティ監視/監査の重要性

情報システムのセキュリティ維持に関して、
セキュリティの監視/監査が非常に重要



監視／監査をすることが大事。

セキュリティ監視のメリット

セキュリティ監視のメリット

(1)不正アクセスの予知、防止ができる。

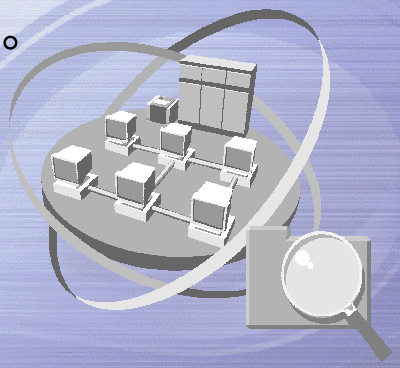
(2)ネットワーク設定ミスを防止できる。

(3)内部犯罪の防止ができる。

(4)監視データを元に

・セキュリティの脅威分析

・対策立案ができる。



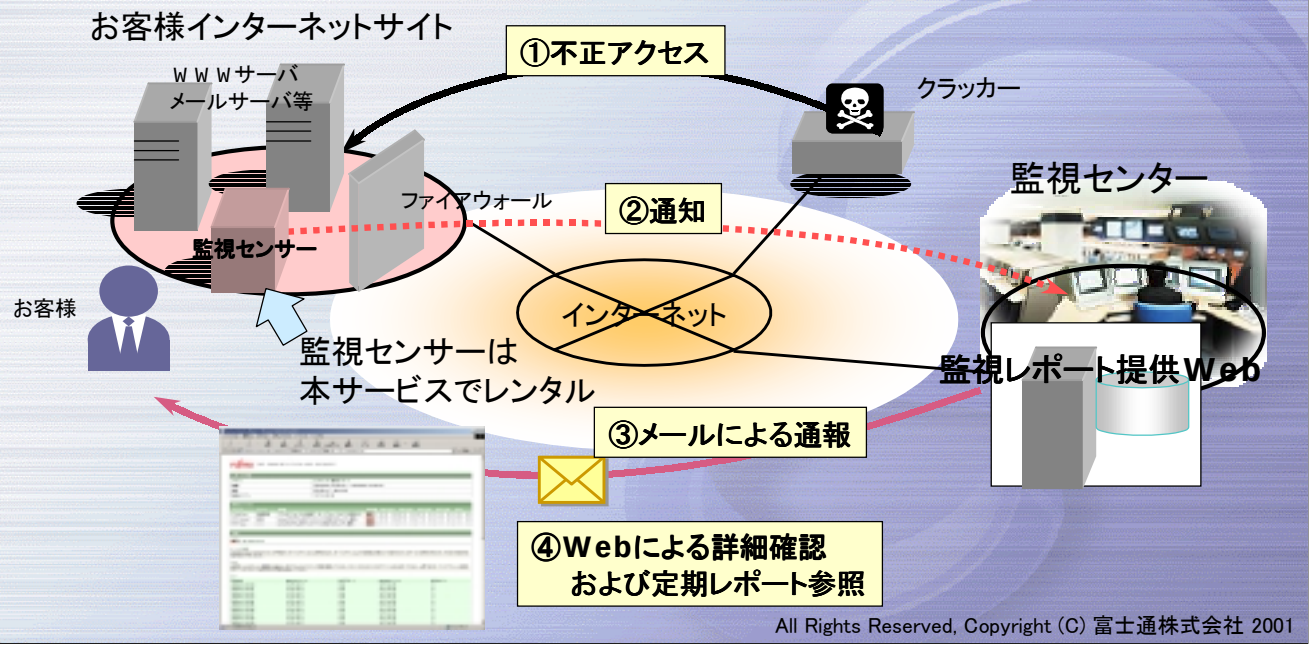
特に中小規模のシステムにおいては、
セキュリティ対策として「監視」の導入を推奨。
(費用対効果が大きい)

システムの不正アクセスの兆候を積極的にとらえる。

セキュリティ監視サービス　エコノミー

□「富士通ネットワーク監視センター」より、お客様インターネットサイトを24時間365日監視し、クラッカーによる不正アクセスをe-mailにより、迅速に通知。

□お客様専用Webサイトを参照することで、1月間の不正アクセス詳細レポートを確認。

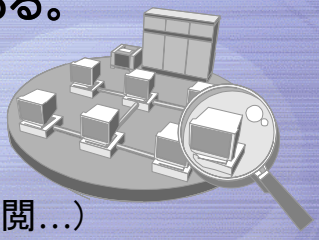


１５万／月というサービスを２００１年５月から提供している。

セキュリティ監査の必要性

セキュリティ監査

システム面及び運用/体制面(人的, 物理的)での、脆弱な部分を、明確にし、不正の早期発見及びその抑制に効果がある。



監査ログの取得と不正侵入の発見

・各種ログ監査(ネットワーク,OS, アプリケーション,メール検閲…)
・擬似アタック

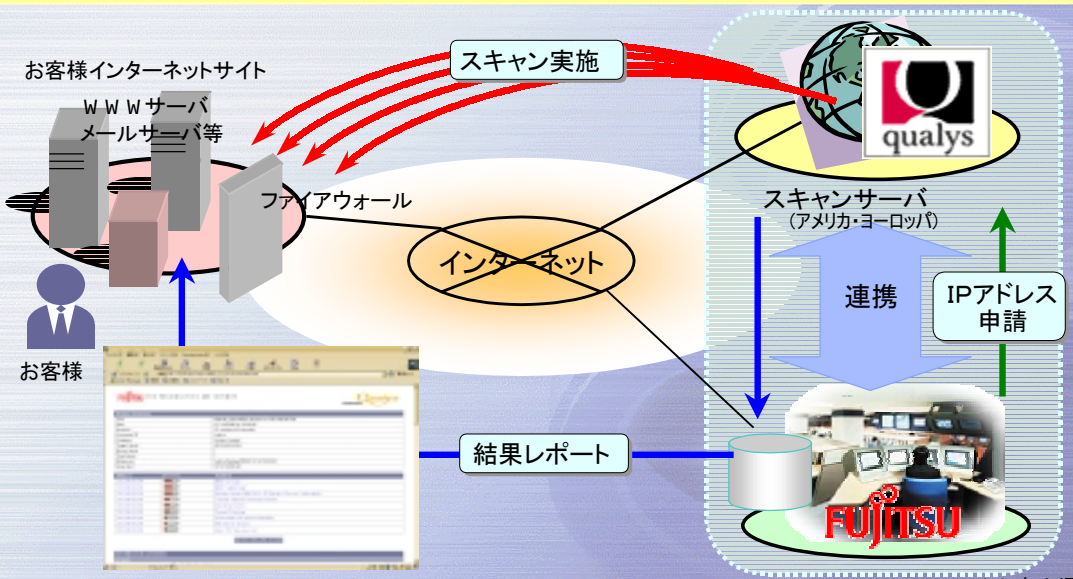
セキュリティポリシーの運用状態の監視

・組織面/運用面の監査

セキュリティホールは、実際にアタックしてみることが分かり易い。

アタックテストサービス エクスプレス

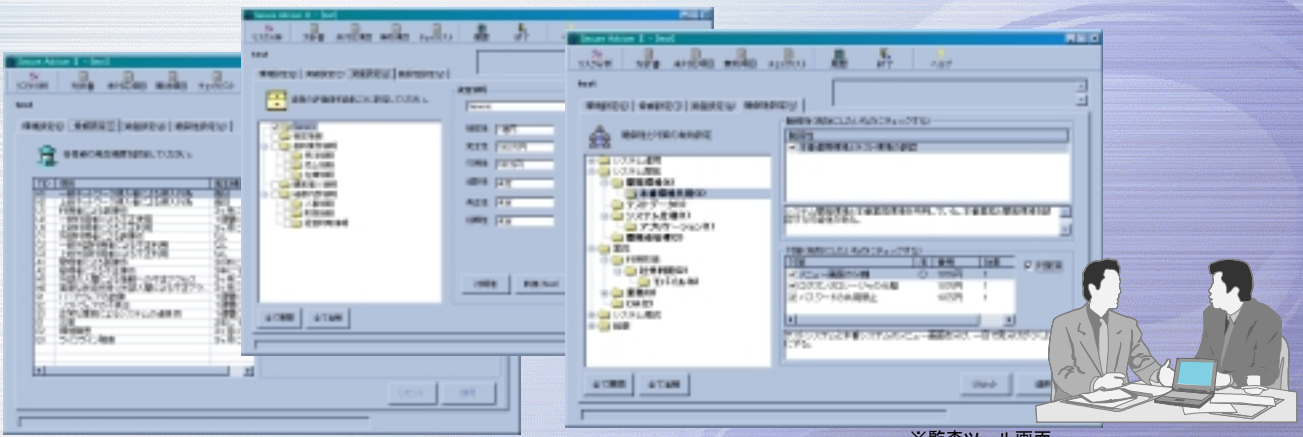
- 世界中で高い評価を受けている、米国Qualys社実施の QualysGuard™によるセキュリティアセスメントサービスを、日本国内で初めて提供。
- 迅速なセキュリティホールへの対応。あらたにセキュリティホールが見つかった場合、原則として1日以内に、該当セキュリティホールを検出するアタックパターンが反映される。
- 高速なスキャニング速度 1サーバあたり、(15～20分程度)



25万／年で回数無制限にアタックできる。セキュリティホールへの追従が早い(原則1日以内)のも特長。

セキュリティ評価診断サービス

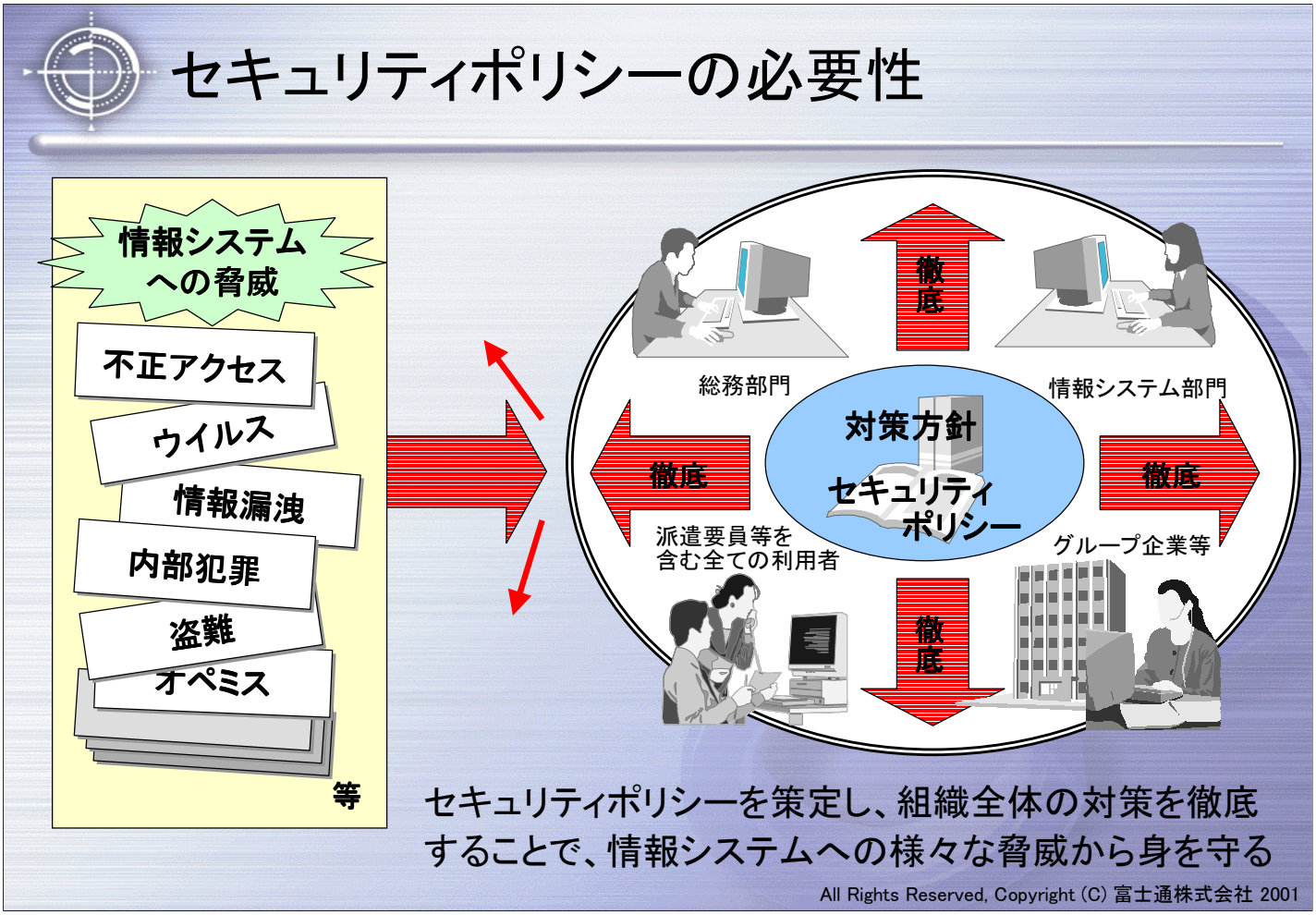
□お客様のインターネットサイトのセキュリティレベルを、客観的に評価し、
より強固なインターネットサイト構築のための技術的・組織的指針を、短期間で提供



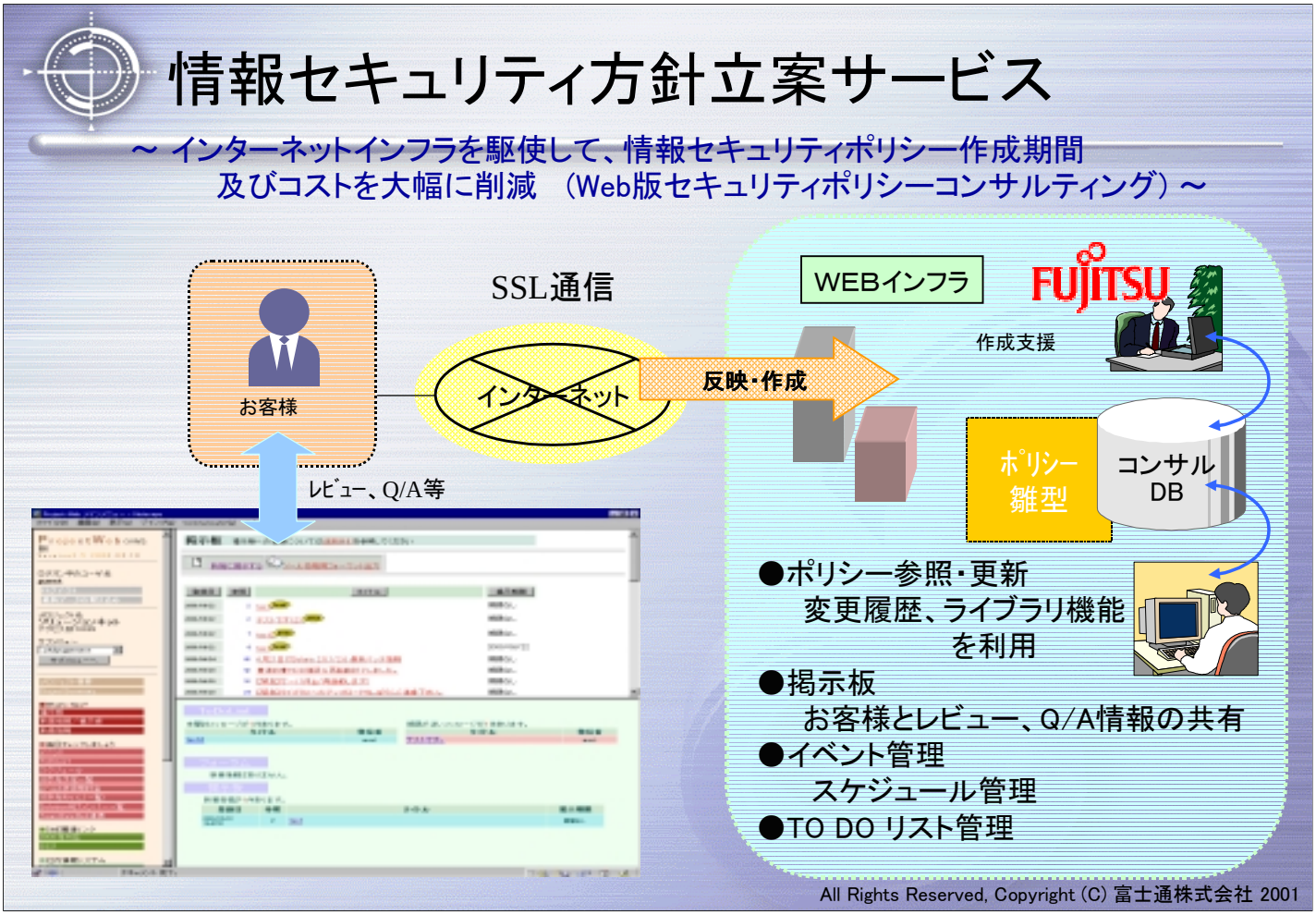
※監査ツール画面

■対面ヒアリングにより、インターネット接続環境を客観的に監査
■システム系以外の、組織面・運用面からの脆弱性を診断
■具体的なセキュリティ対策の基礎情報、セキュリティ方針をアウトプット

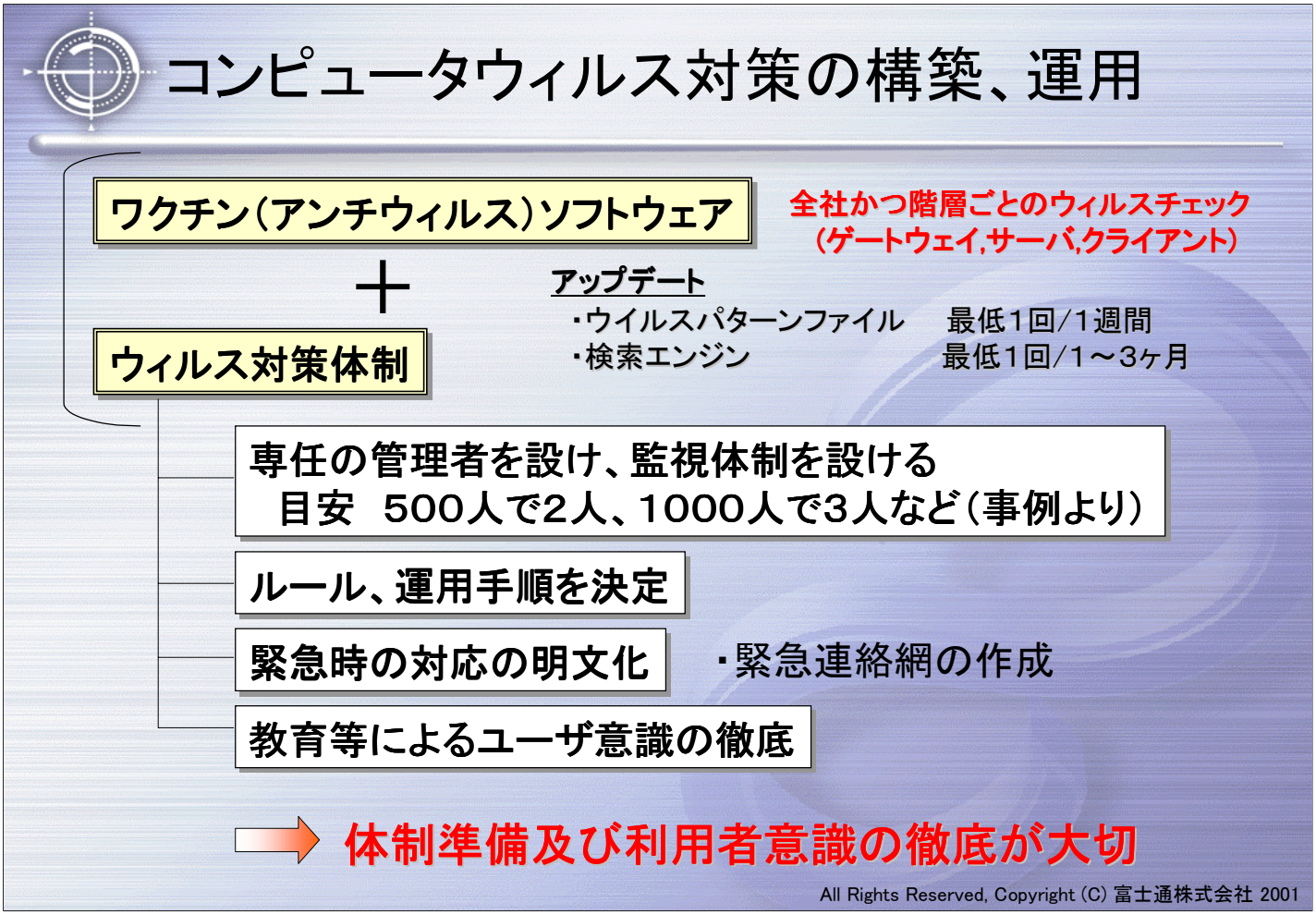
セキュリティがルール通り運用されていることを監査する。専用ツールにより約2週間で監査することが可能。



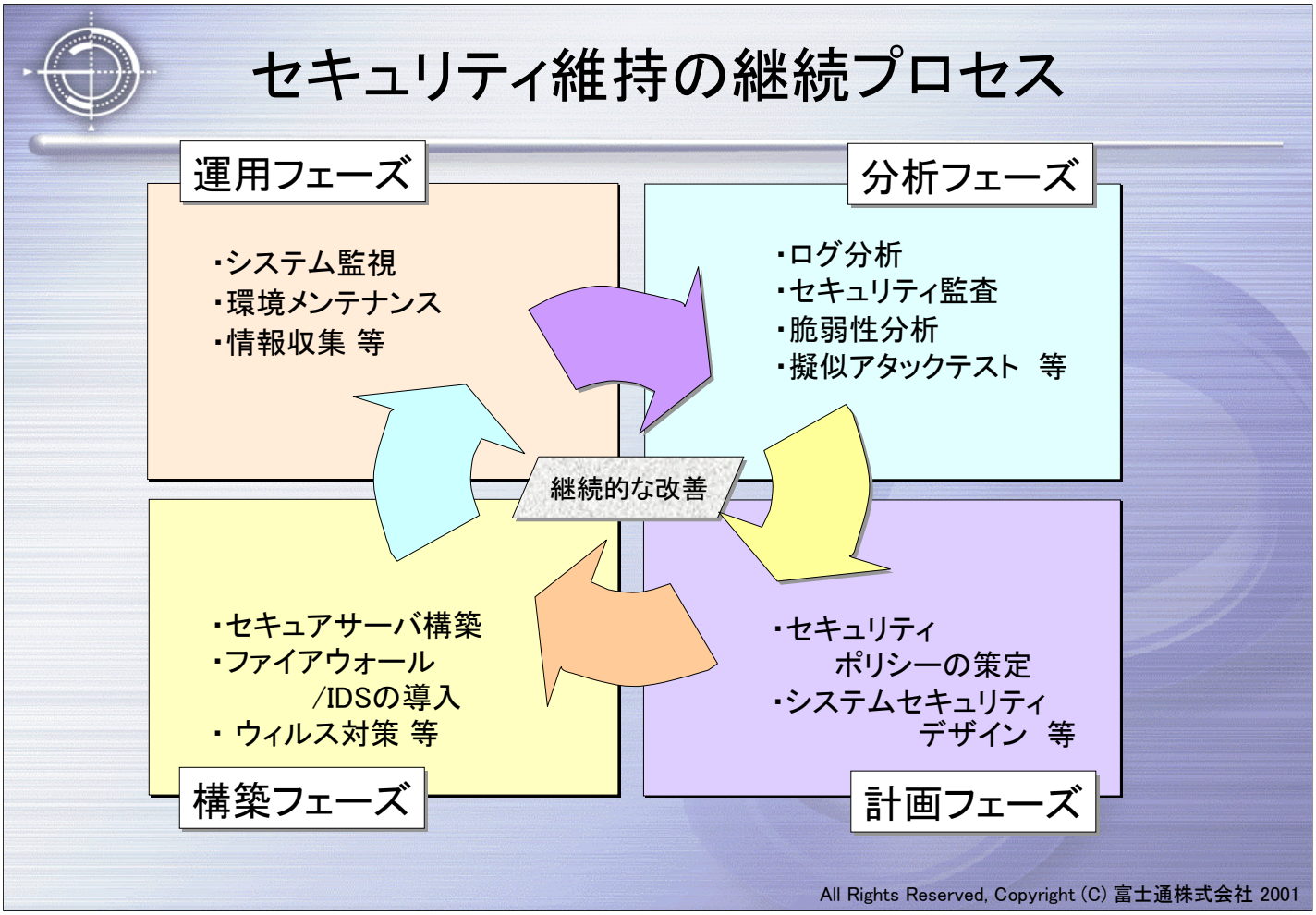
組織的な対応が大事。インタネットは特に重要。



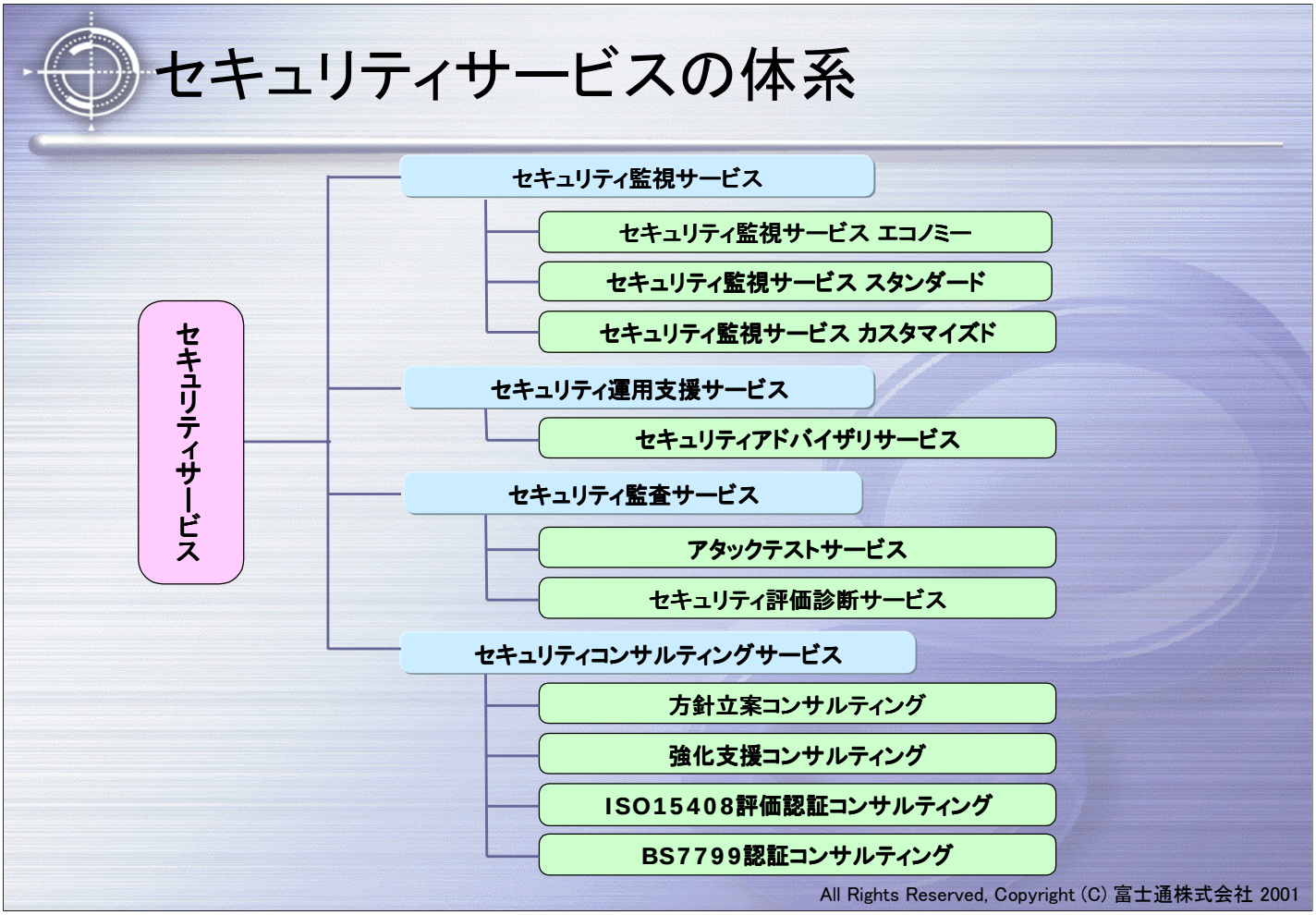
ポリシーのひな型をベースにネットワークでコミュニケーションし、カストマイズ。
約1カ月でセキュリティポリシーを作成することが可能。



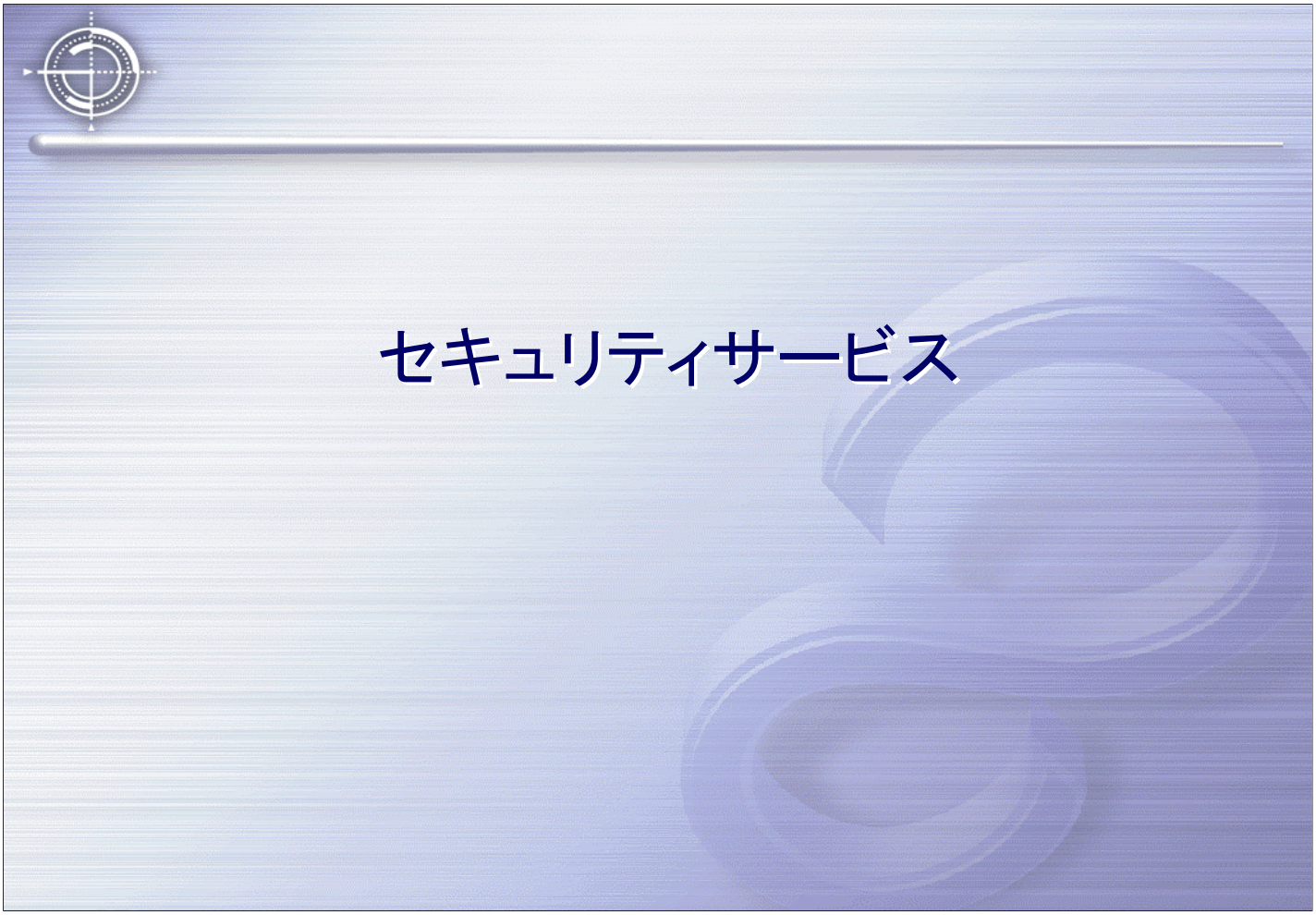
ウィルス対策も対策ソフトを入れることが基本だが、感染したときに被害を拡大させないための体制や管理も重要。



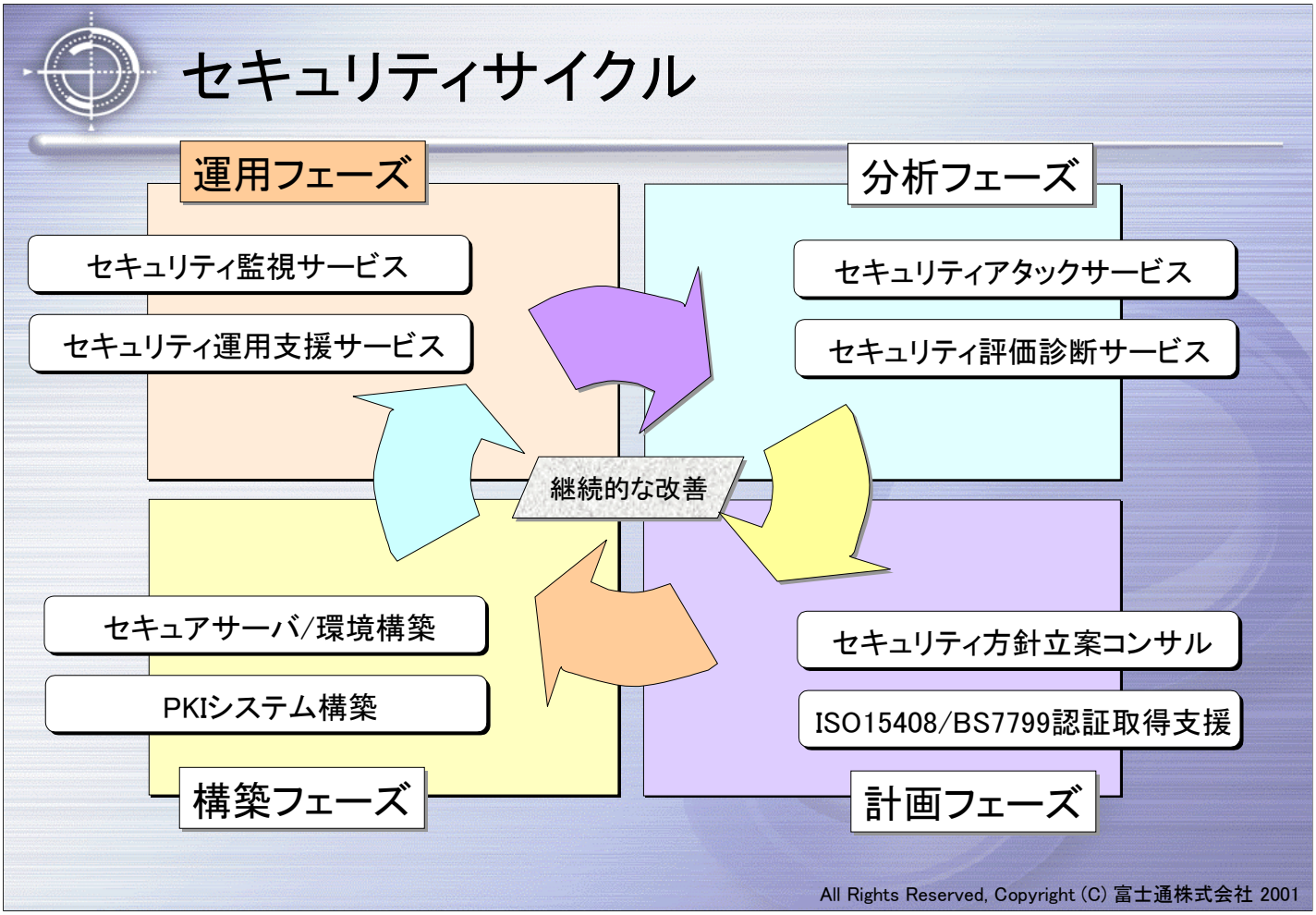
一過性ではいけない。改善のプロセスを考えること。



セキュリティ維持のプロセスに沿った体系でサービスを提供。



富士通がご提供するセキュリティのサービスについてご紹介。

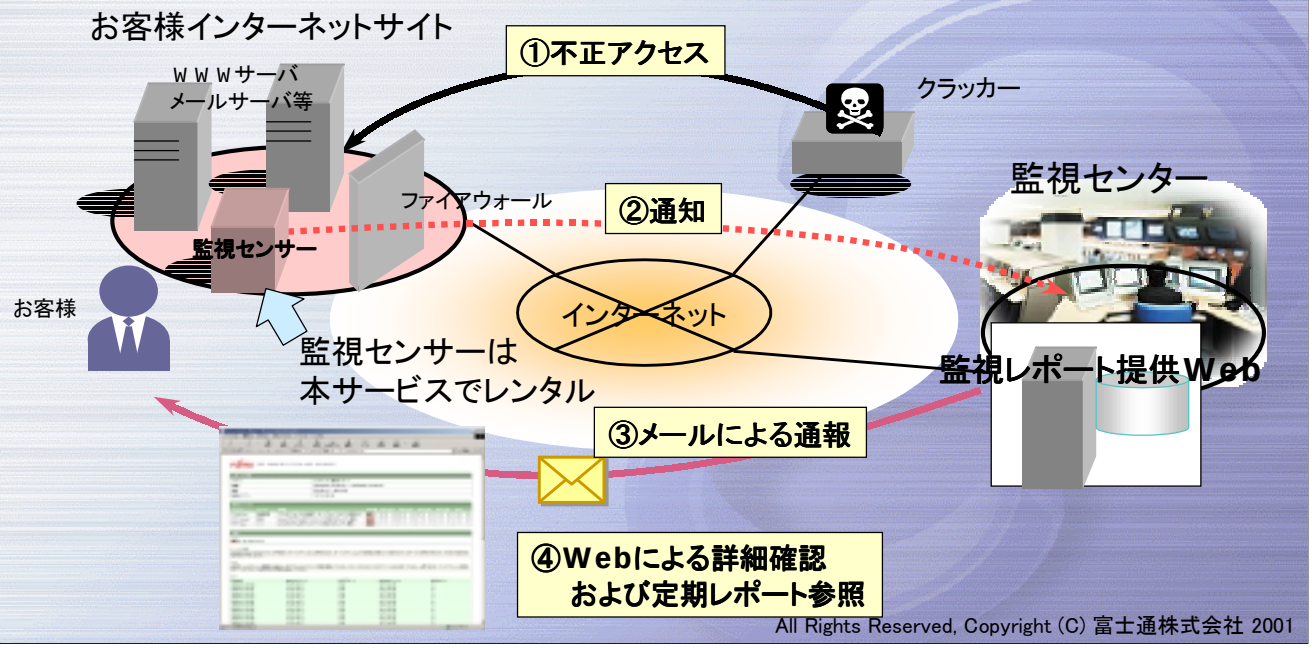


まず、セキュリティを維持・継続するサイクルの運用フェーズの中から、セキュリティ監視サービスについてご紹介。

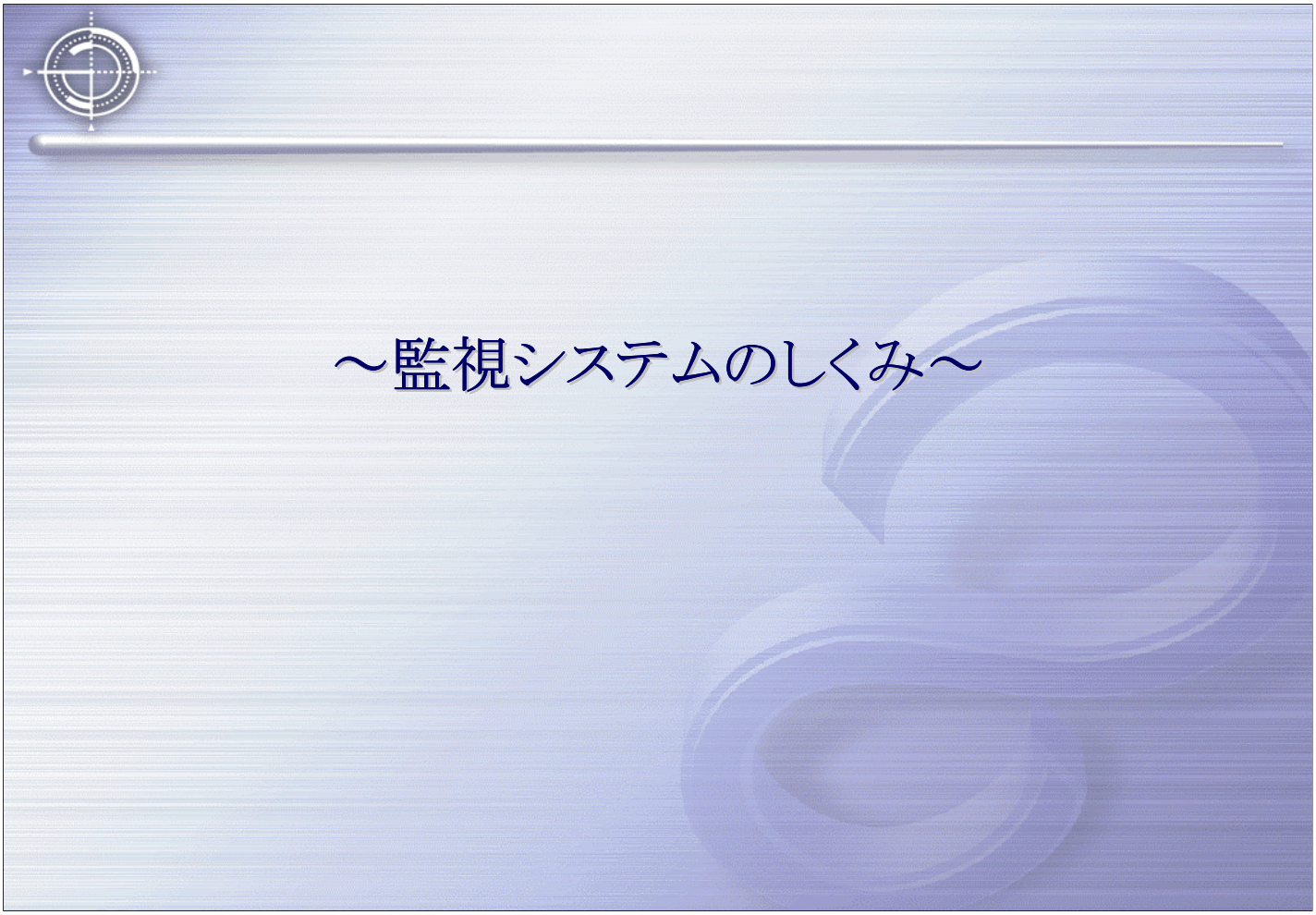
セキュリティ監視サービス　エコノミー

□「富士通ネットワーク監視センター」より、お客様インターネットサイトを24時間365日監視し、クラッカーによる不正アクセスをe-mailにより、迅速に通知。

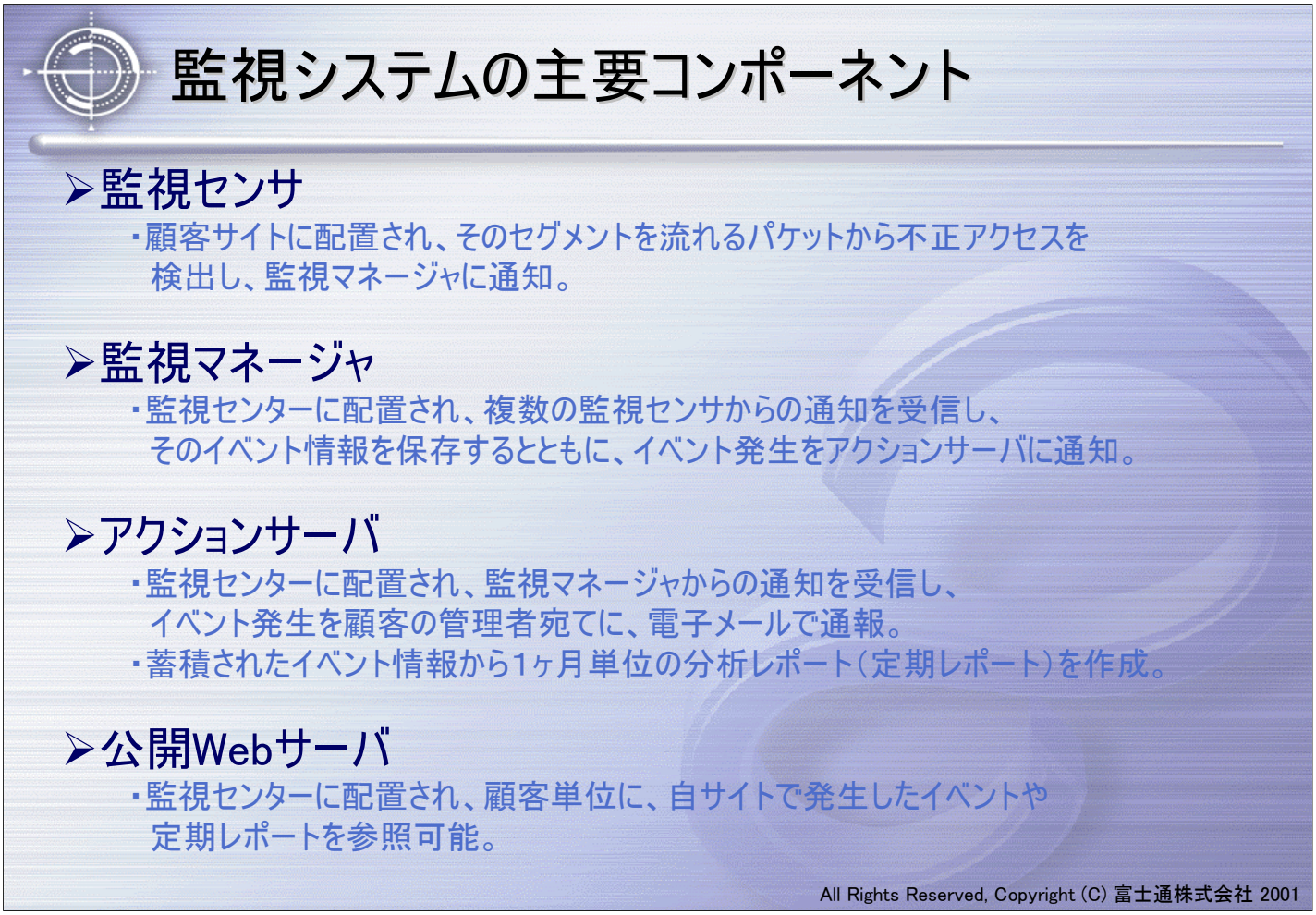
□お客様専用Webサイトを参照することで、1月間の不正アクセス詳細レポートを確認。



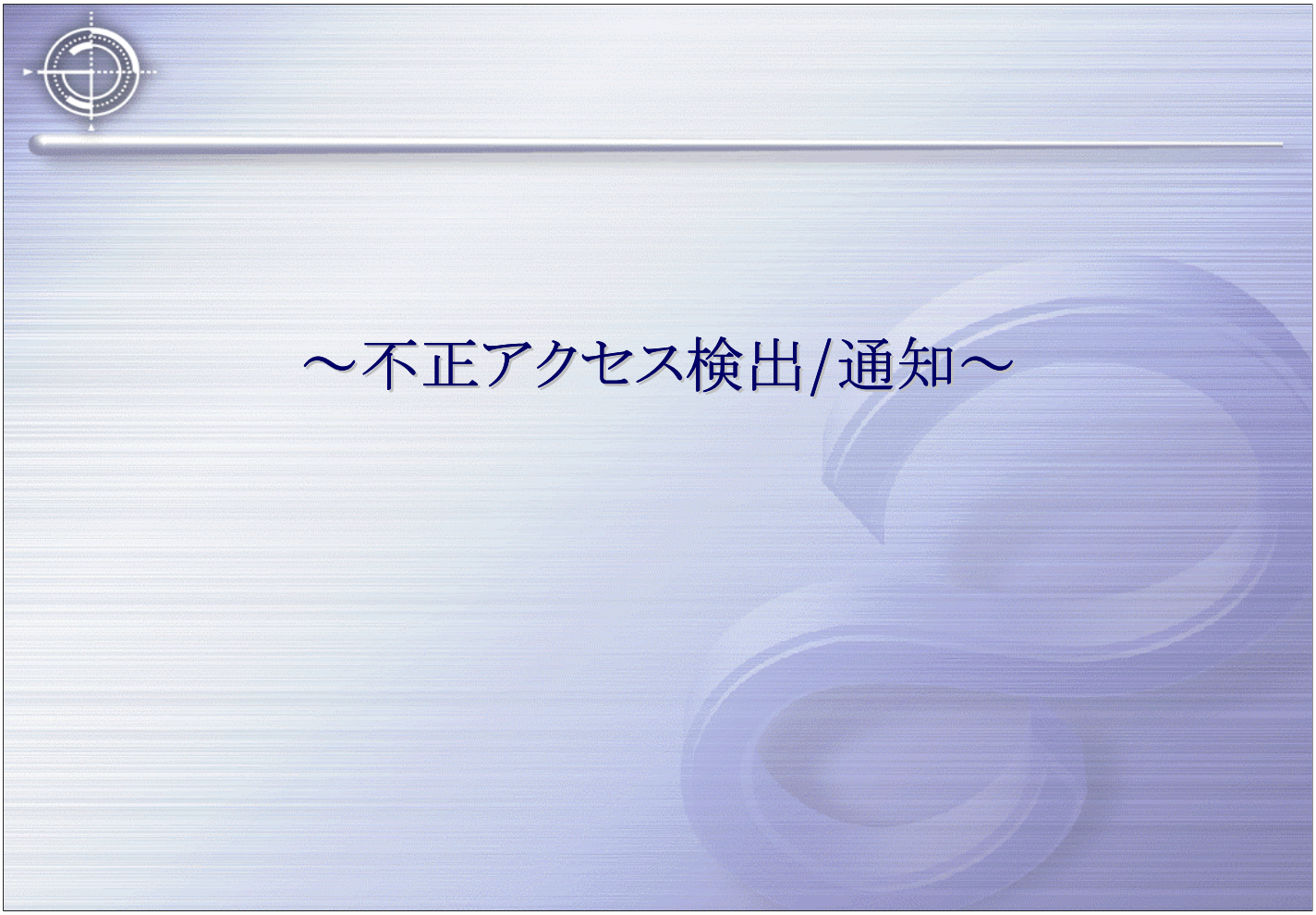
セキュリティ監視サービスの中のエコノミーについてご紹介。
・24時間365日の機械監視。
・ご契約いただいたお客様には専用のWebサイトをご提供。
・不正なアクセス検出時には、E-Mailでご通知。詳細状況はお客様専用のWebサイトからご提供。
・毎月一ヶ月間のイベント発生状況の定期レポートをお客様専用のWebサイトからご提供。



セキュリティ監視サービスエコノミーのシステムについてご説明。

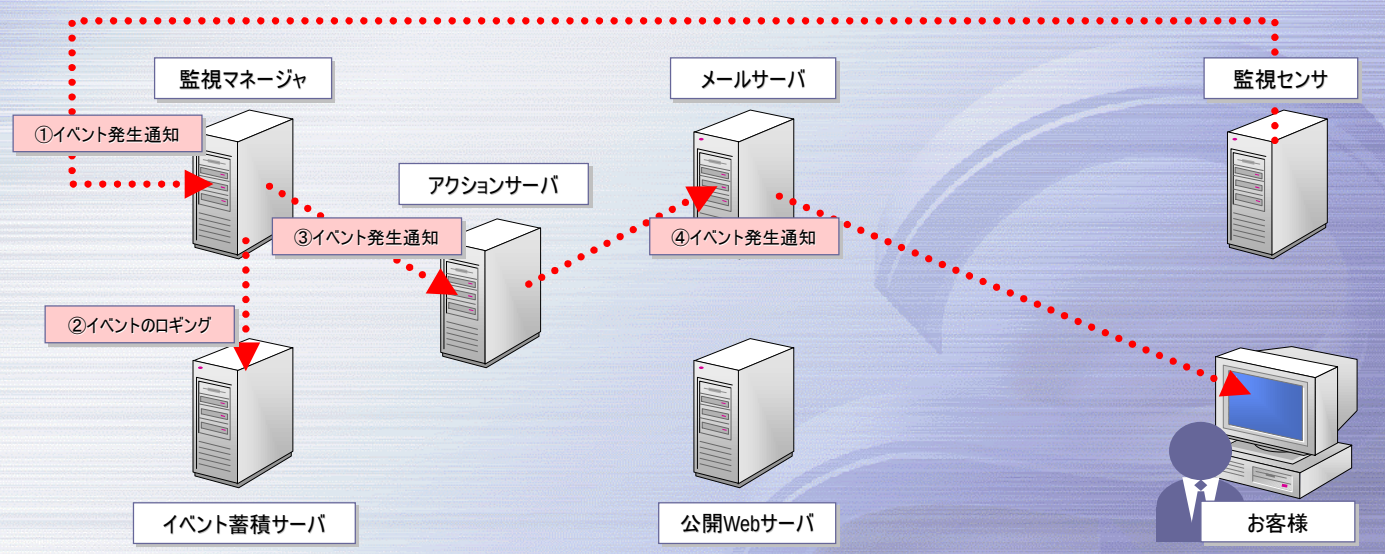


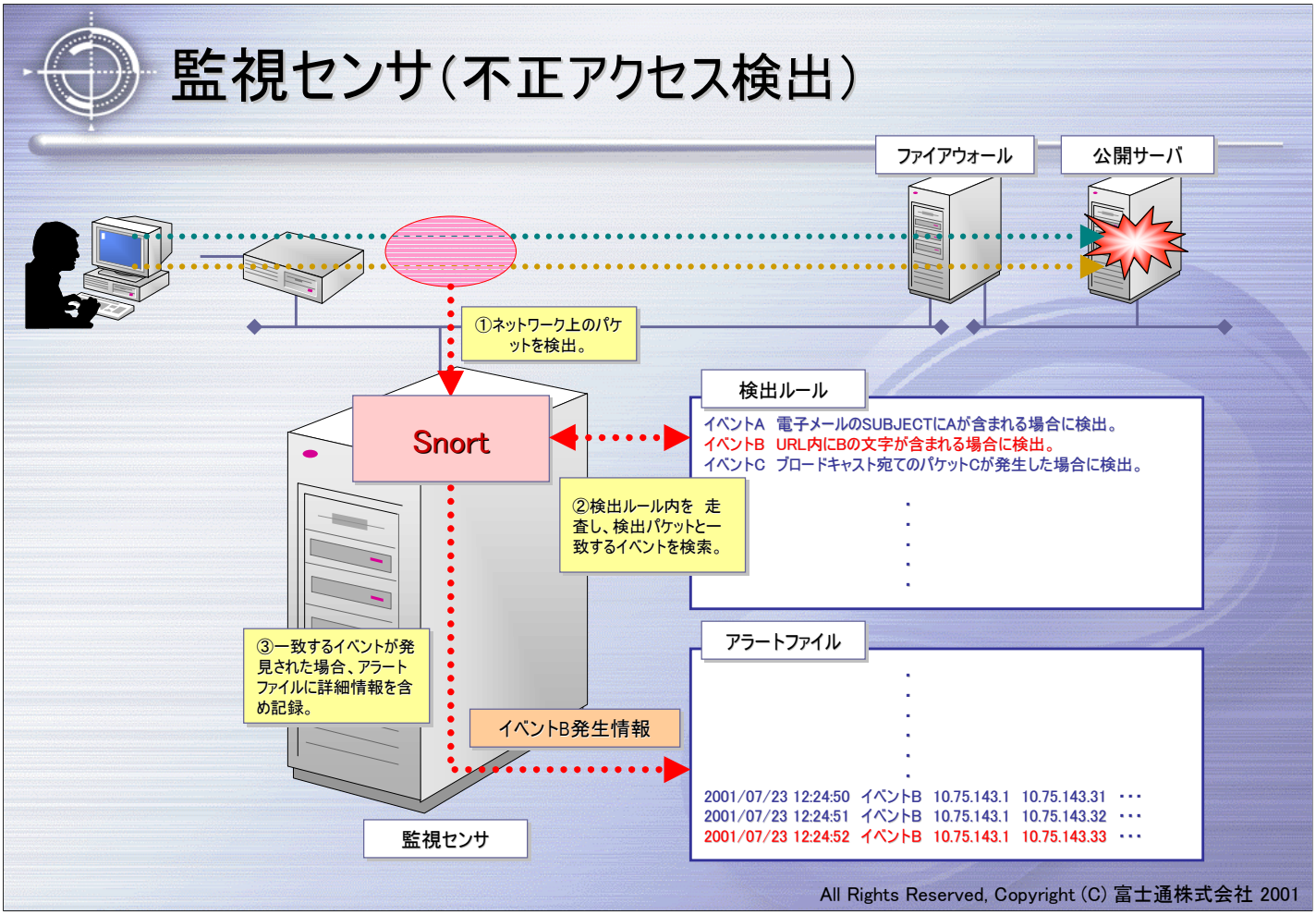
システムの主要なコンポーネントは、
・監視センサ
・監視マネージャ
・アクションサーバ
・公開Webサーバ
の四つ。

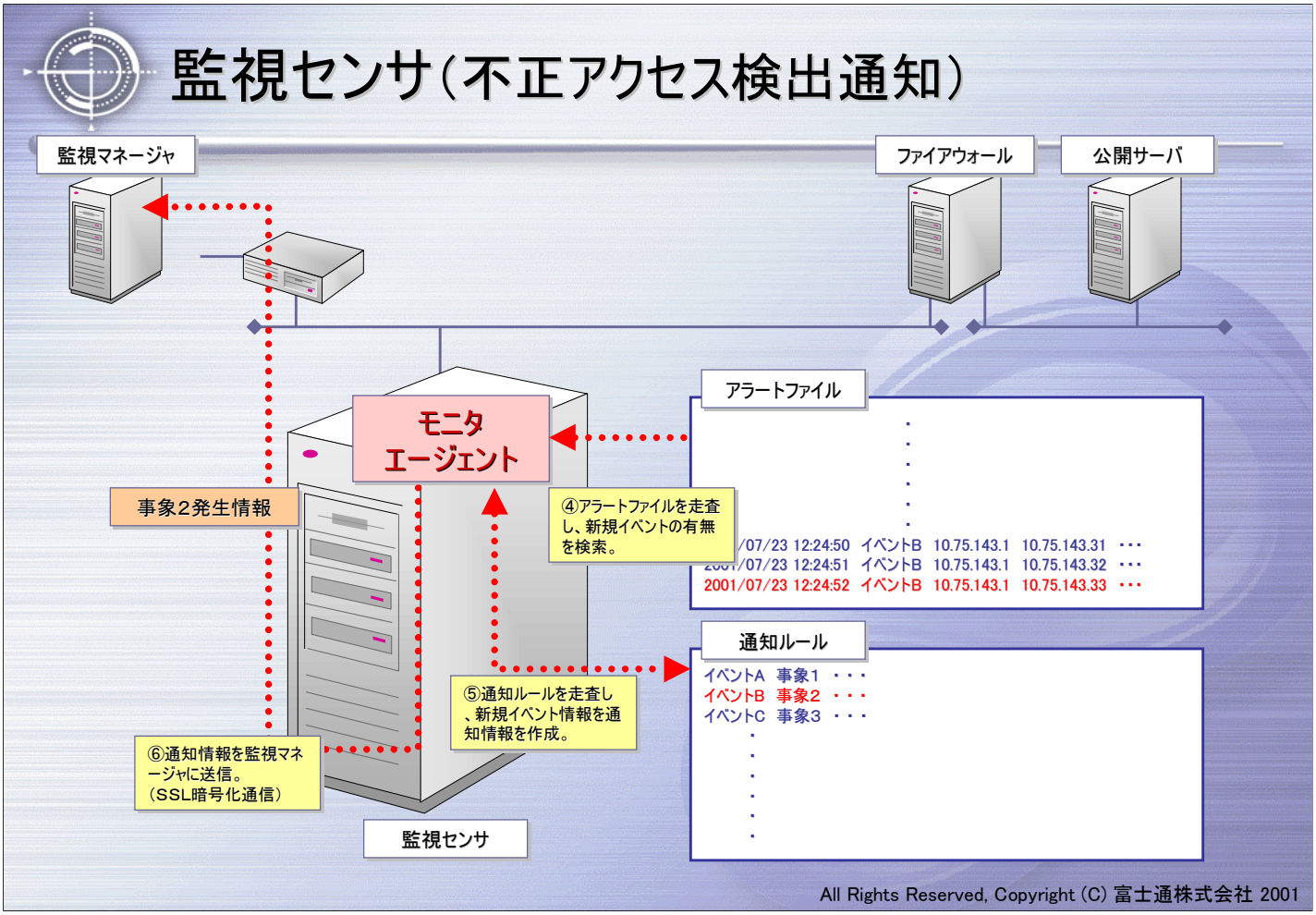


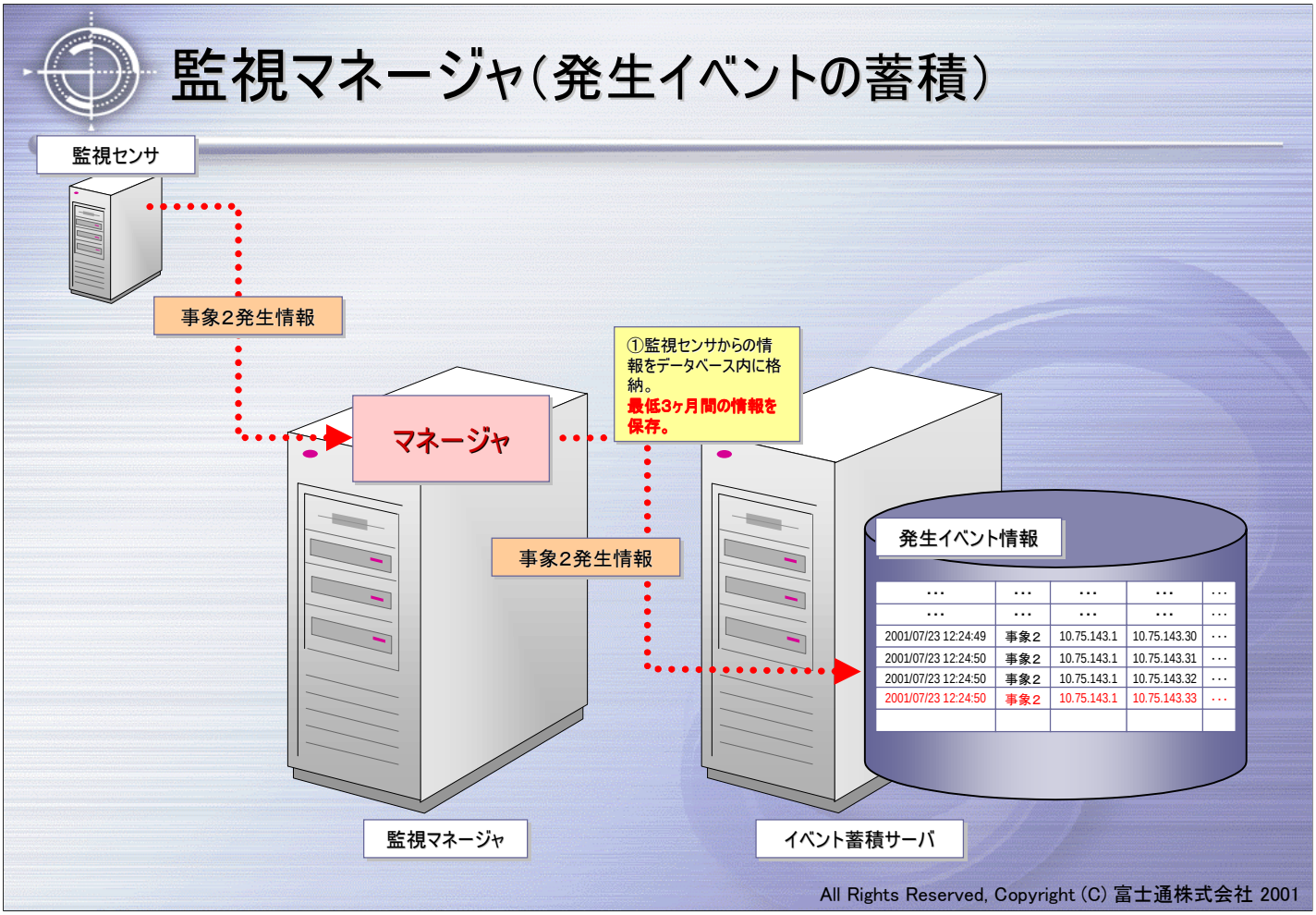
不正アクセスの検出/通知に関するシステム的ご説明。

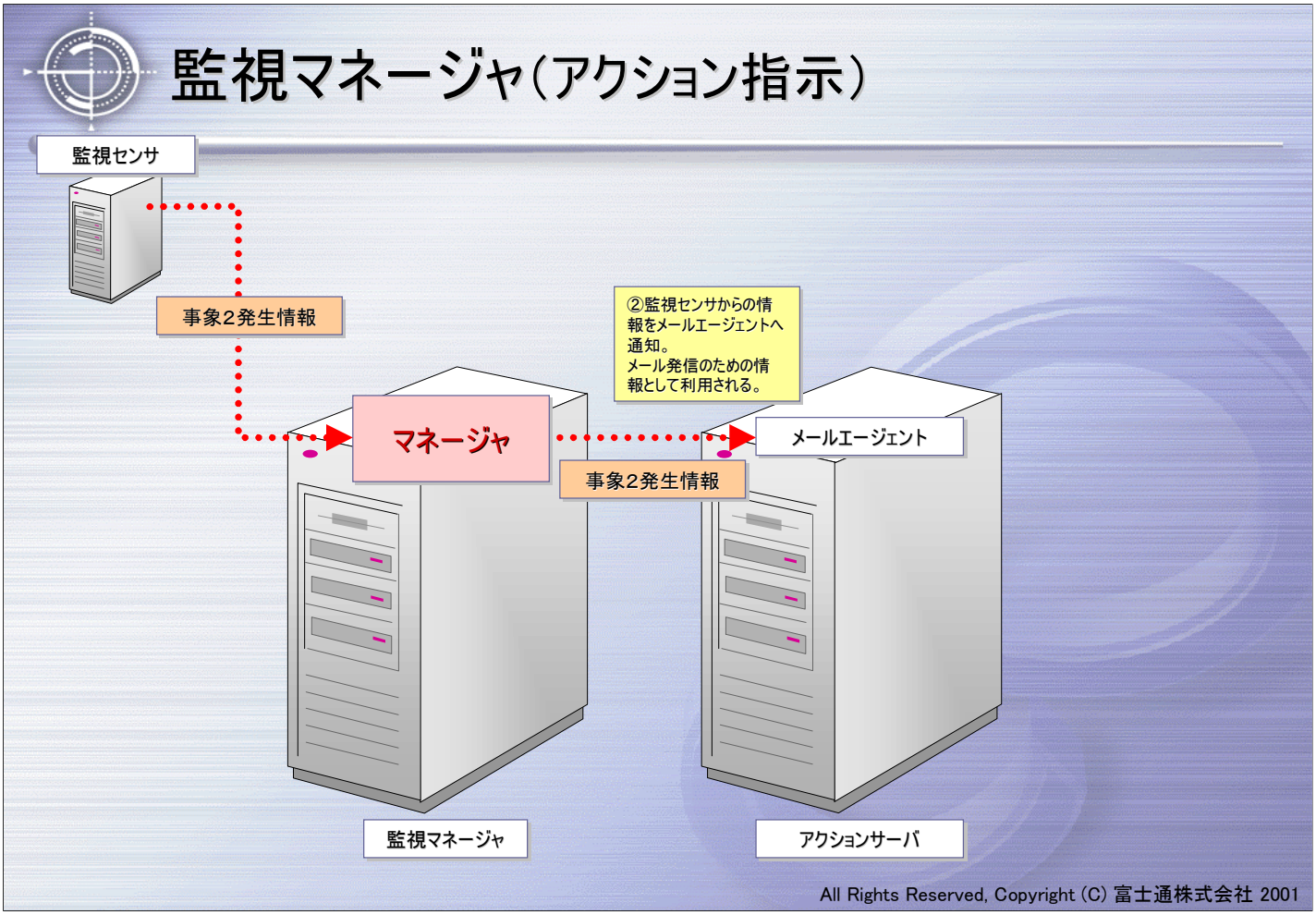
サービス フロー概要

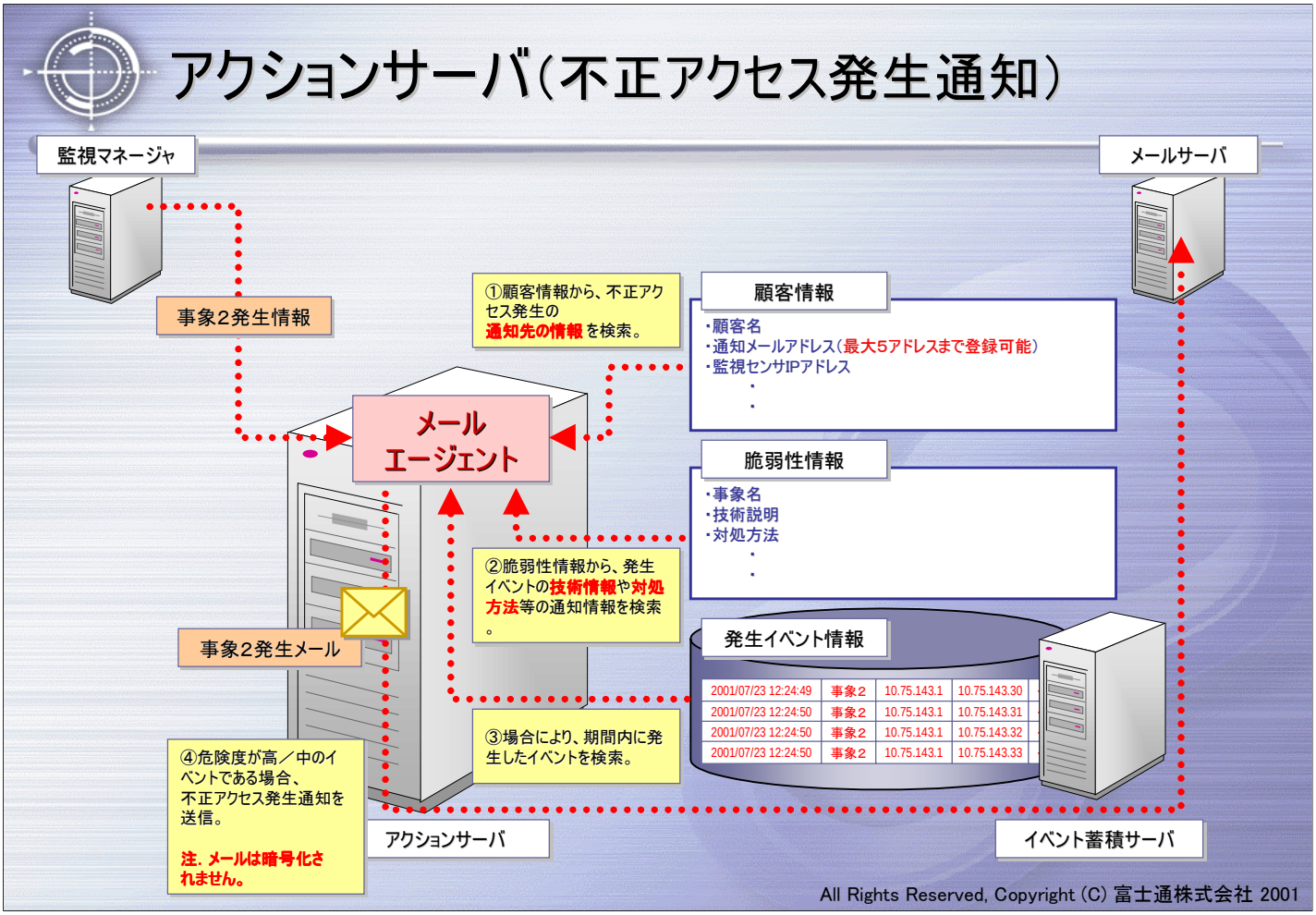


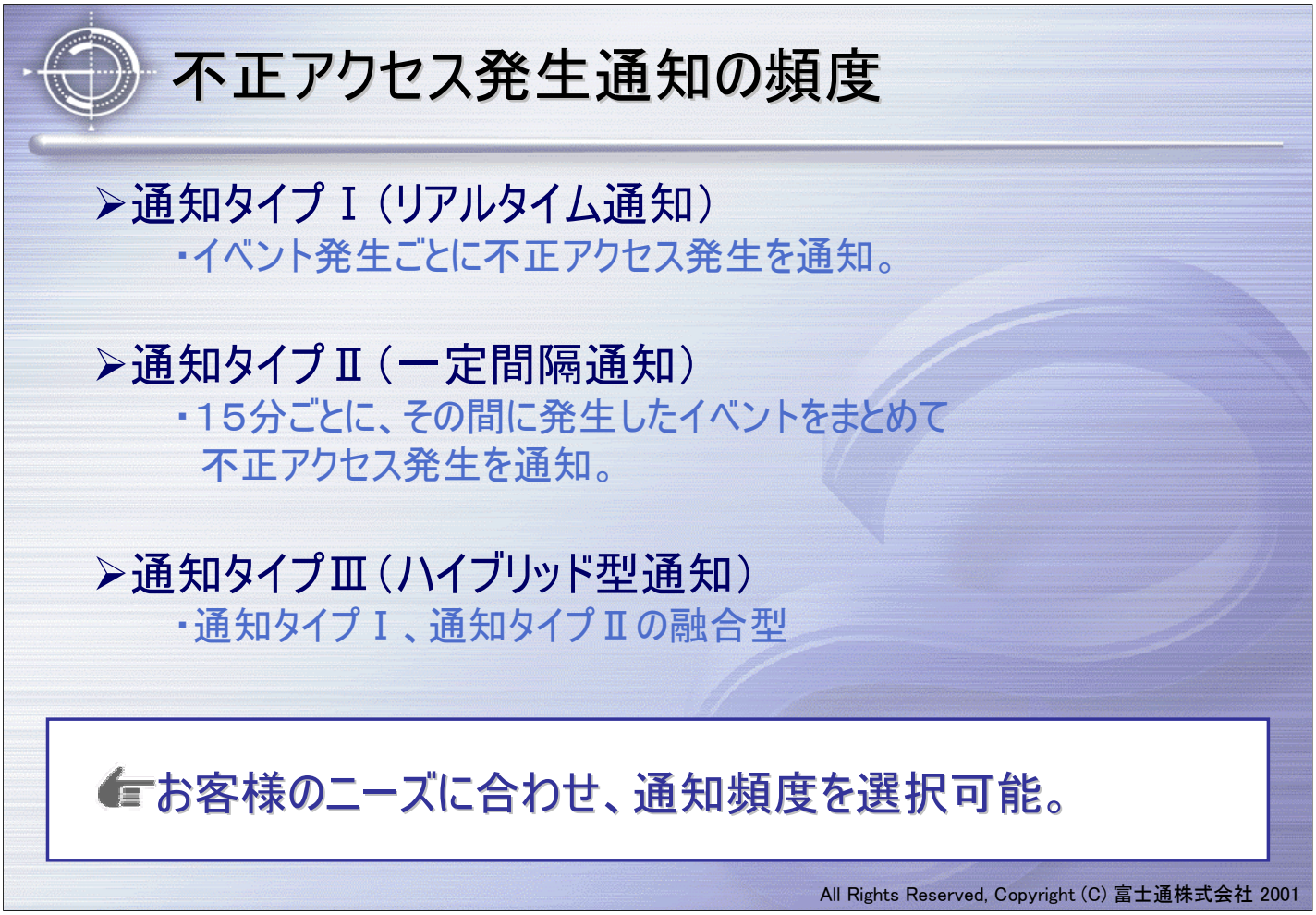




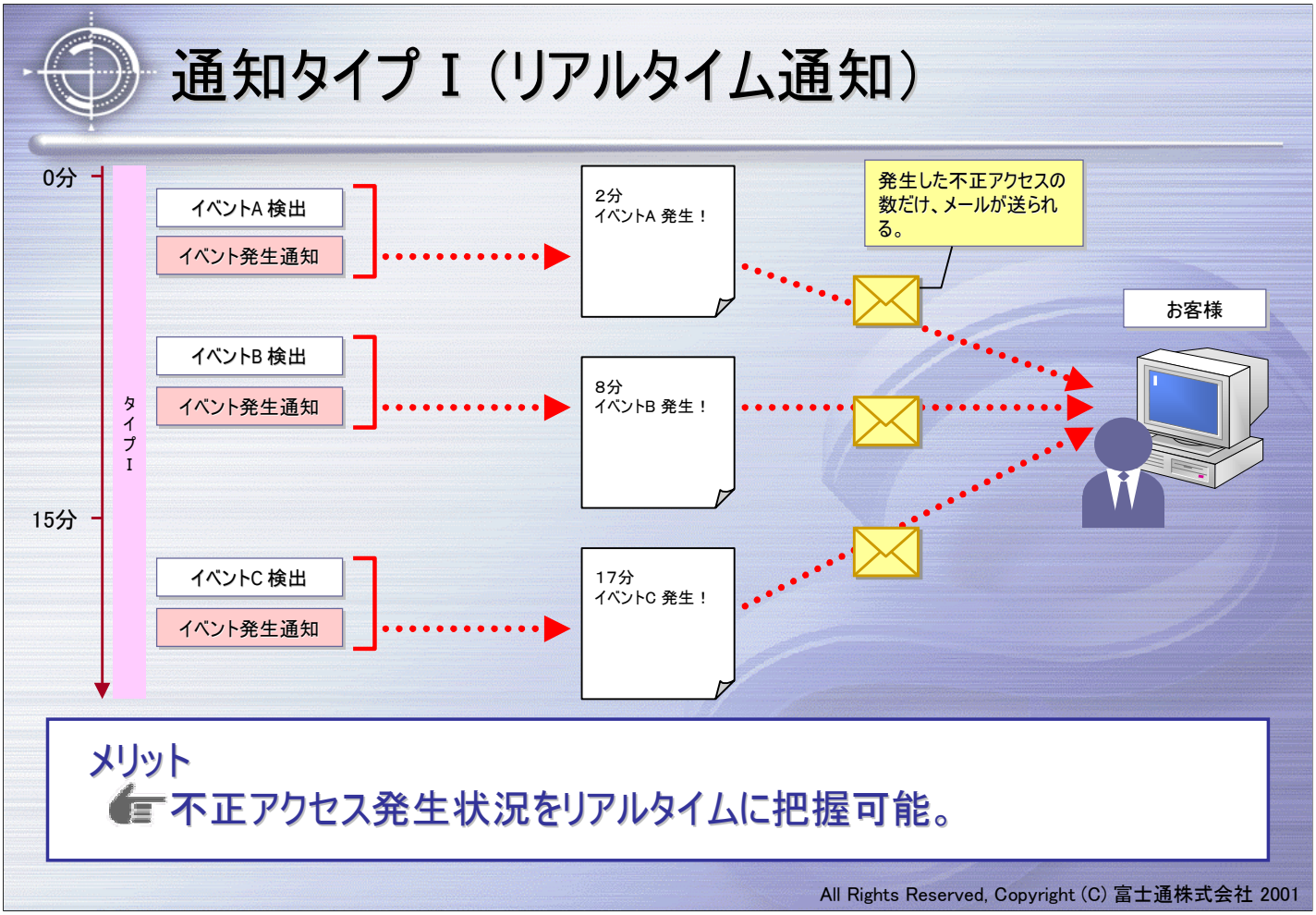




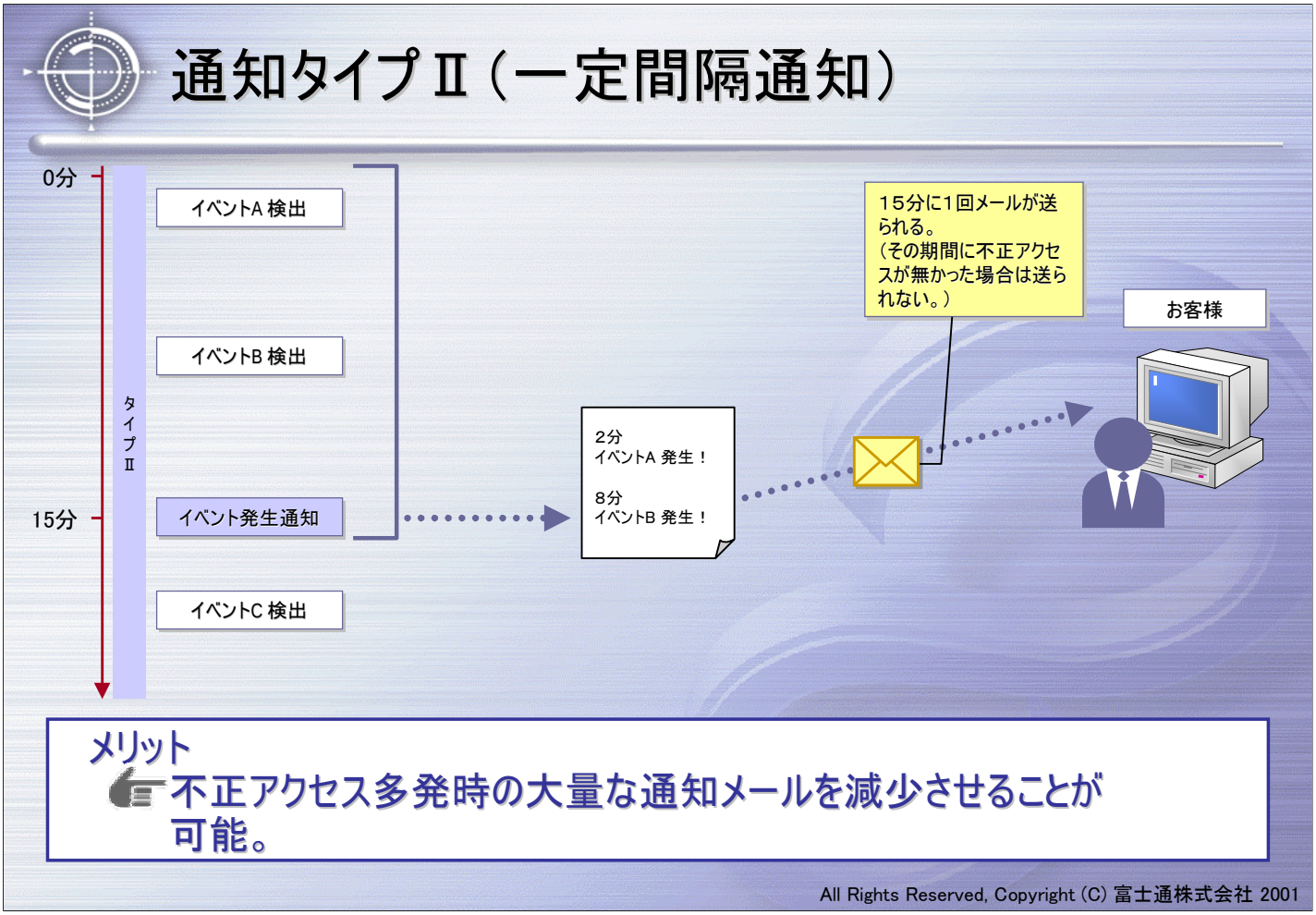




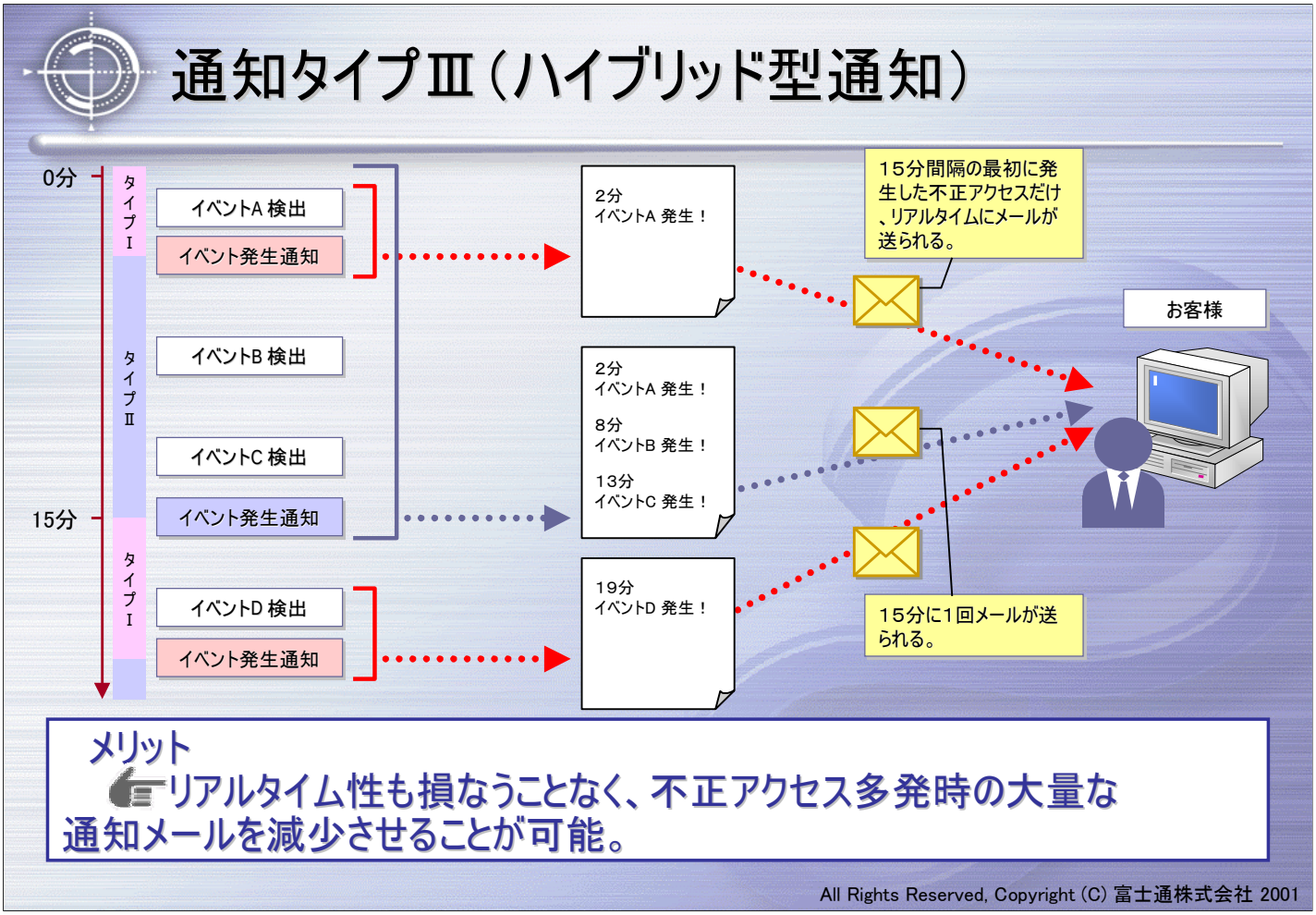
不正アクセスを検出した時のE-Mail送信頻度は、お客様のニーズにあわせて三つのタイプからお選びいただける。



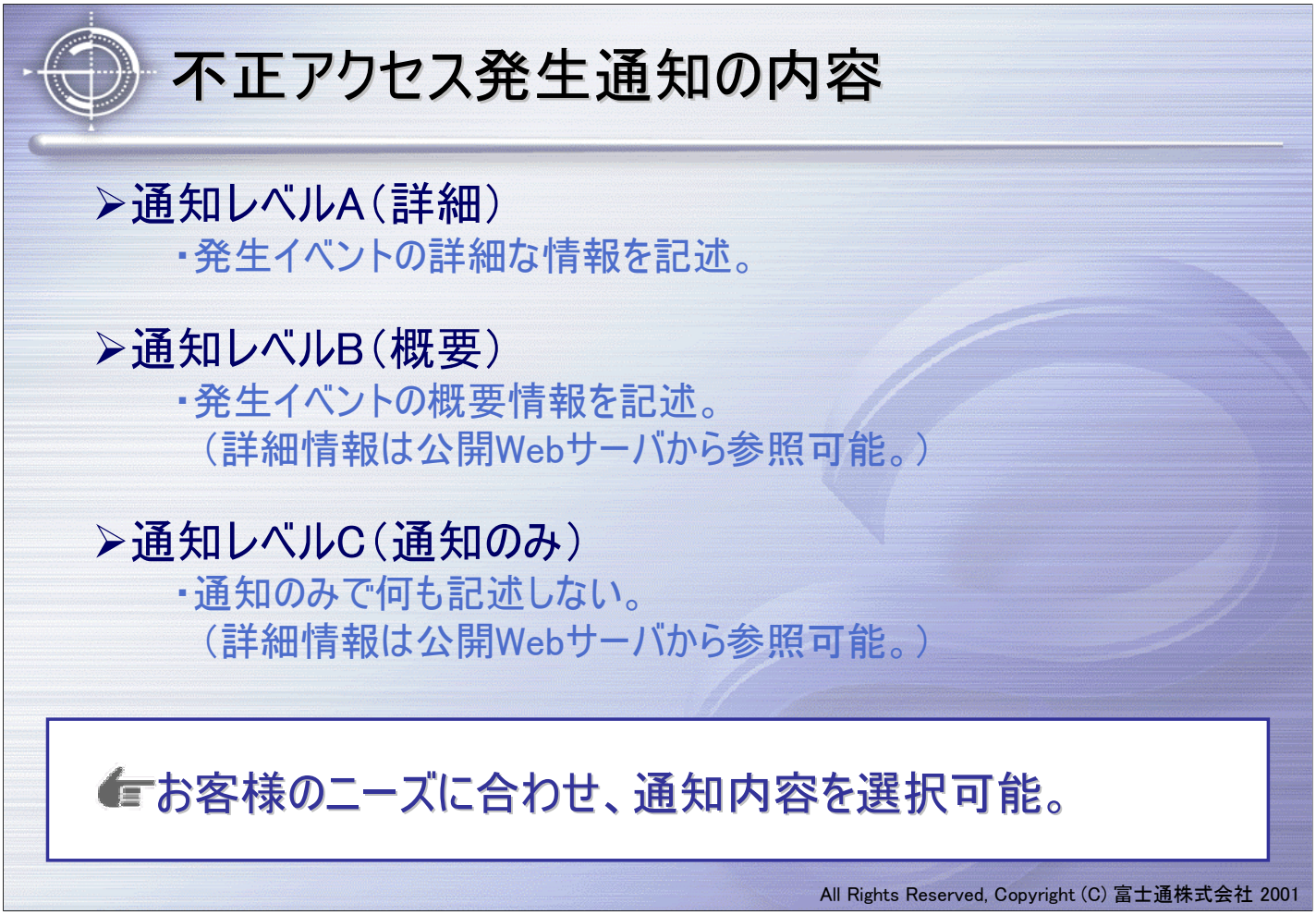
リアルタイム通知。イベント発生時、即時に通知。
・メリット
　・不正アクセスの発生状況をリアルタイムに把握可能なこと。
・デメリット
　・不正アクセスが連続的に行われたときに、通知メールが大量に送信される。



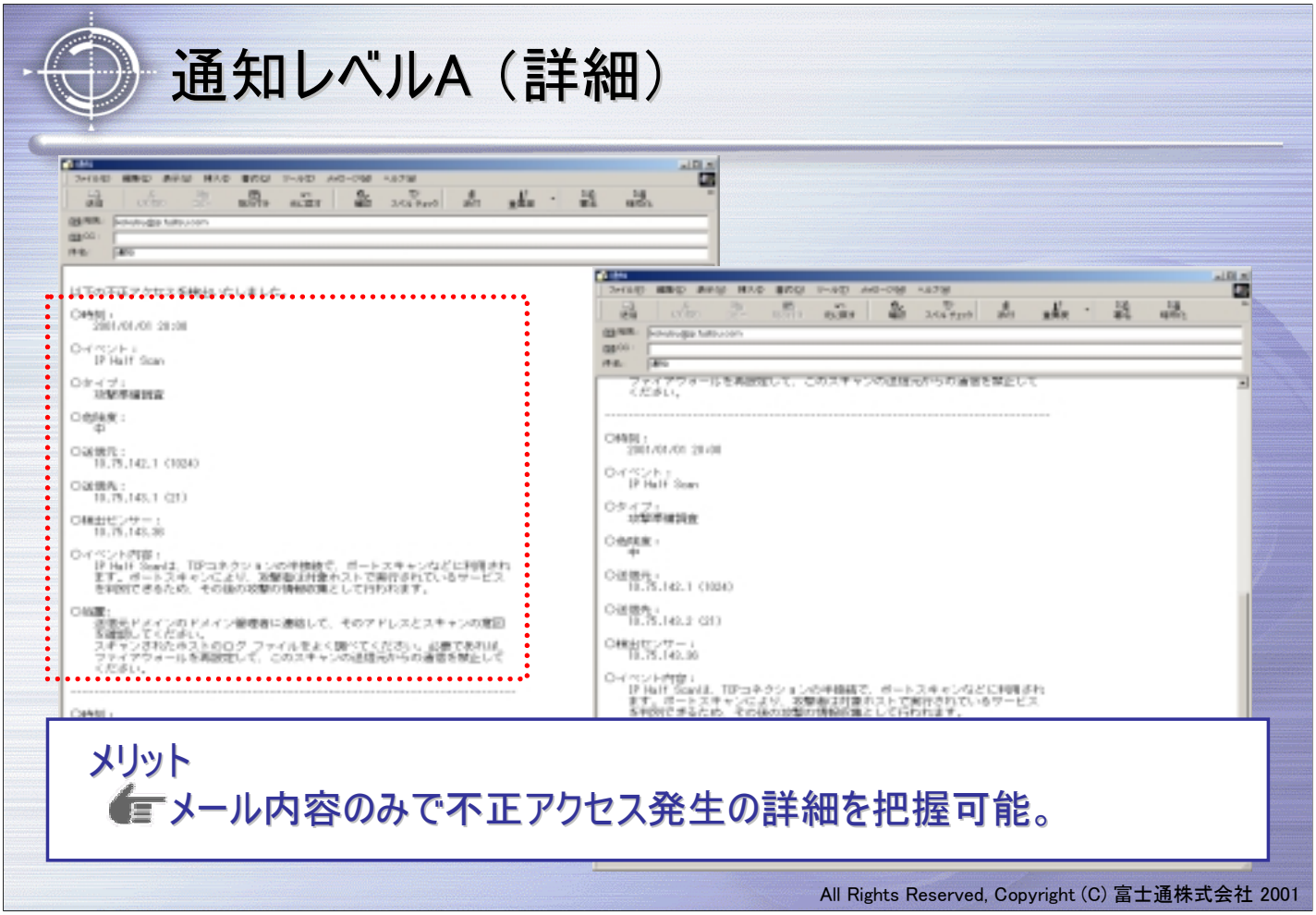
一定間隔通知。15分ごとにその時間内に発生したイベントをまとめて通知。
・メリット
　・不正アクセス多発時の大量な通知メールを減少させることができる
・デメリット
　・不正アクセスを場合によっては15分後でないと知ることができない



ハイブリッド型の通知。通常はリアルタイム通知であるが、不正アクセスが発生すると、自動的に一定間隔通知に移行。15分間のイベントをまとめて一回送信したら、自動的にリアルタイム通知に復帰。リアルタイム通知と、一定間隔通知の両方のメリットを持つ。

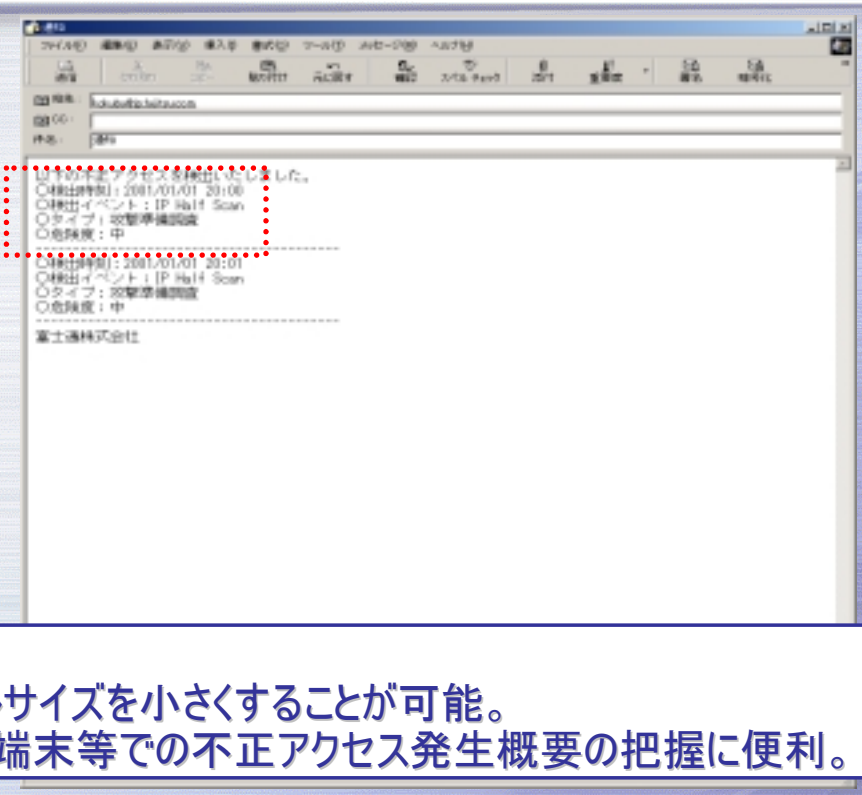


不正アクセス発生時の通知メールの内容は、お客様のニーズにあわせて三つのタイプからお選びいただける。



発生したイベントの詳細な内容を通知。
・メリット
　・メールの内容のみで状況把握が可能。
・デメリット
　・メールが暗号化されないので内容が漏洩する可能性がある。

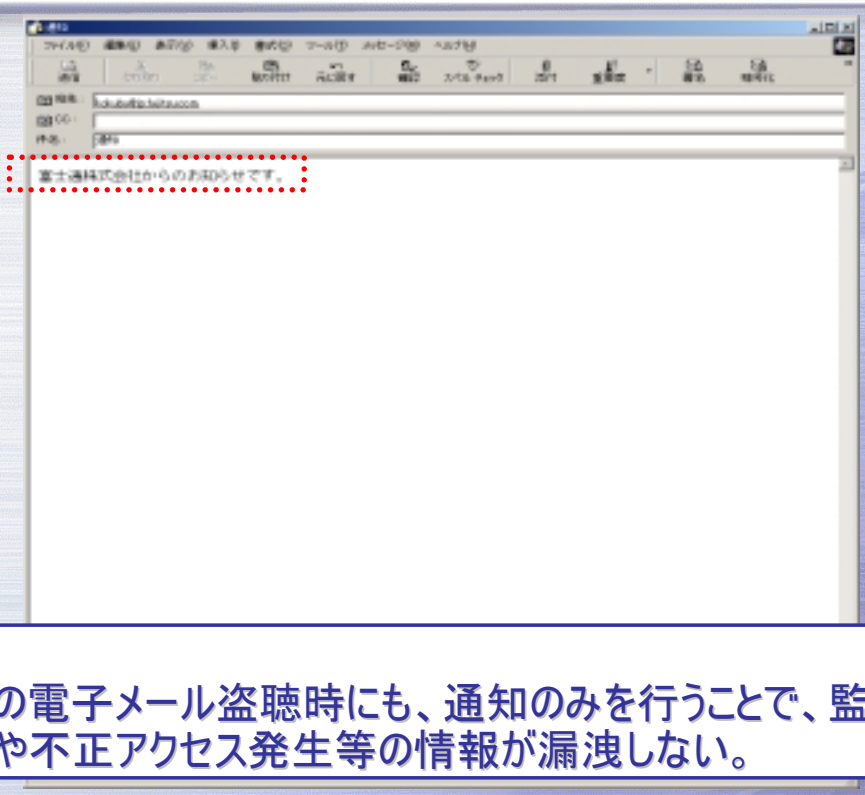
通知レベルB（概要）



メリット
メールサイズを小さくすることが可能。
携帯端末等での不正アクセス発生概要の把握に便利。

発生したイベント内容の概要を通知。
・メリット
　・携帯電話のメールサービスで受信可能。状況の概要を把握することが可能。
・デメリット
　・メールが暗号化されないので内容が漏洩する可能性がある。

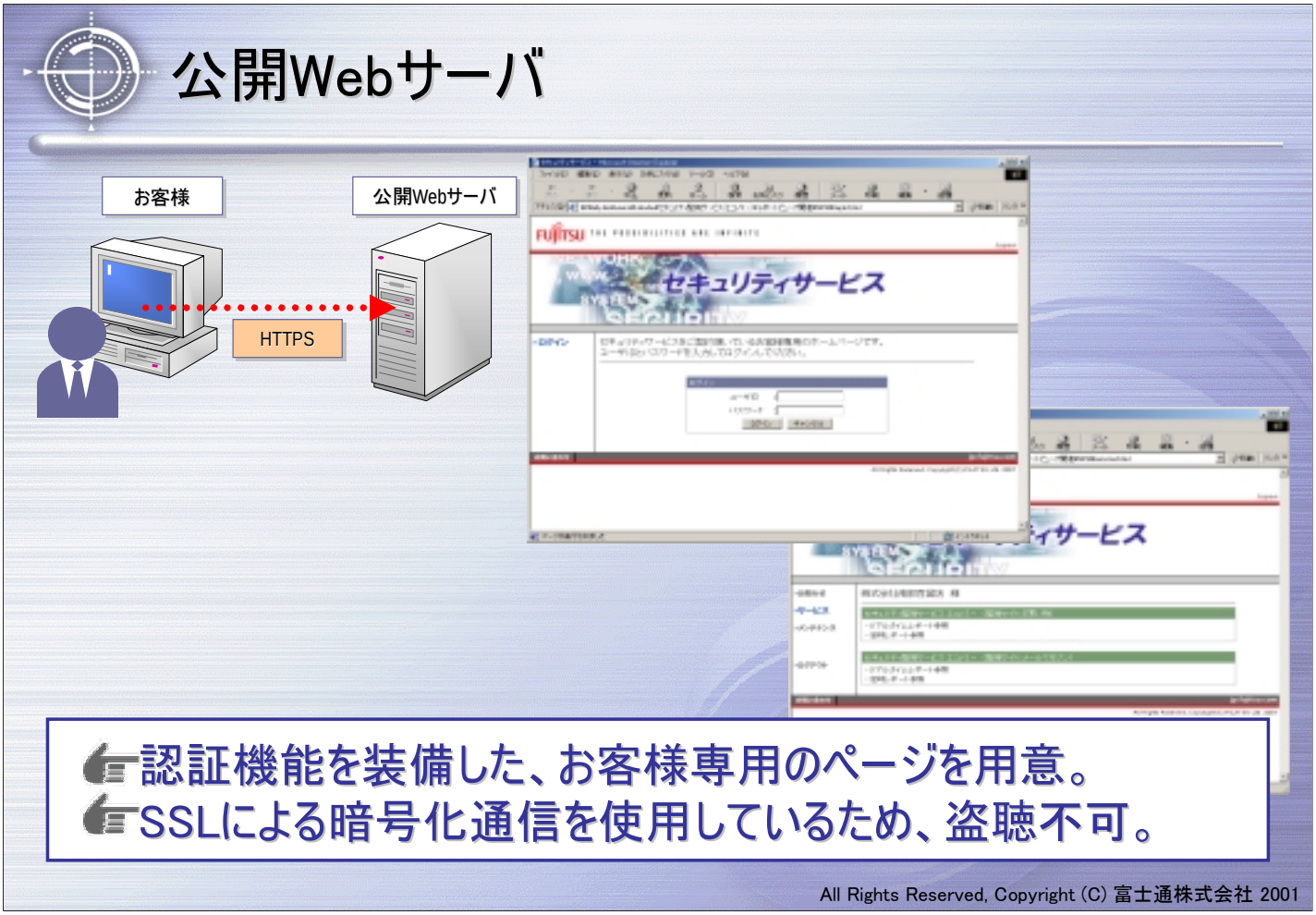
通知レベルC（通知のみ）



メリット

万一の電子メール盗聴時にも、通知のみを行うことで、監視システム導入や不正アクセス発生等の情報が漏洩しない。

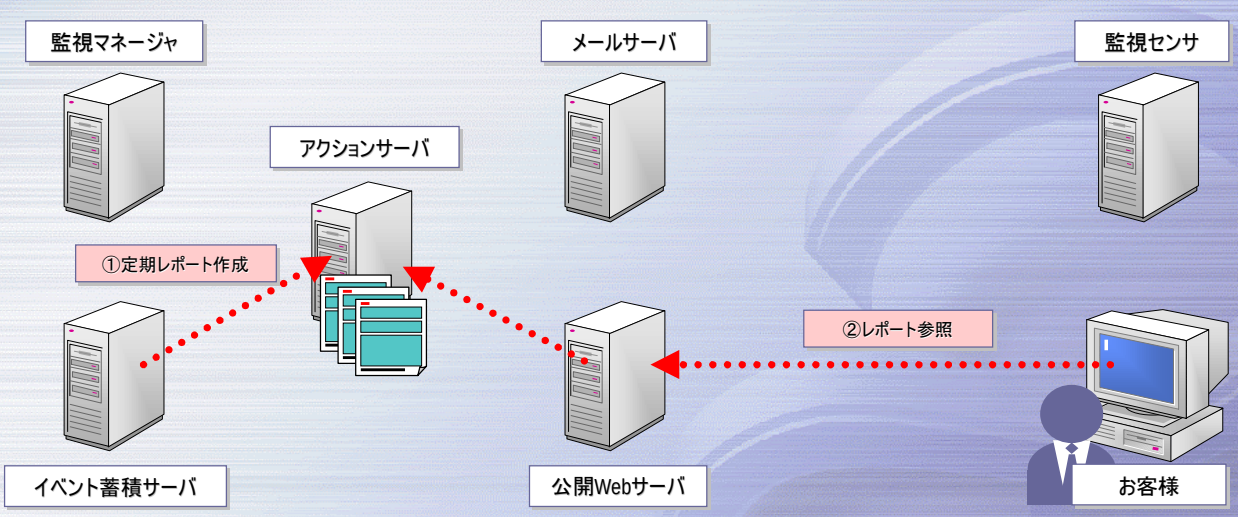
イベントが発生した事実のみを通知。
・メリット
　・万一内容が漏洩しても、被害はほとんどない。
・デメリット
　・メールの内容だけでは状況がわからず、必ずWebにアクセスして状況を確認する必要がある。

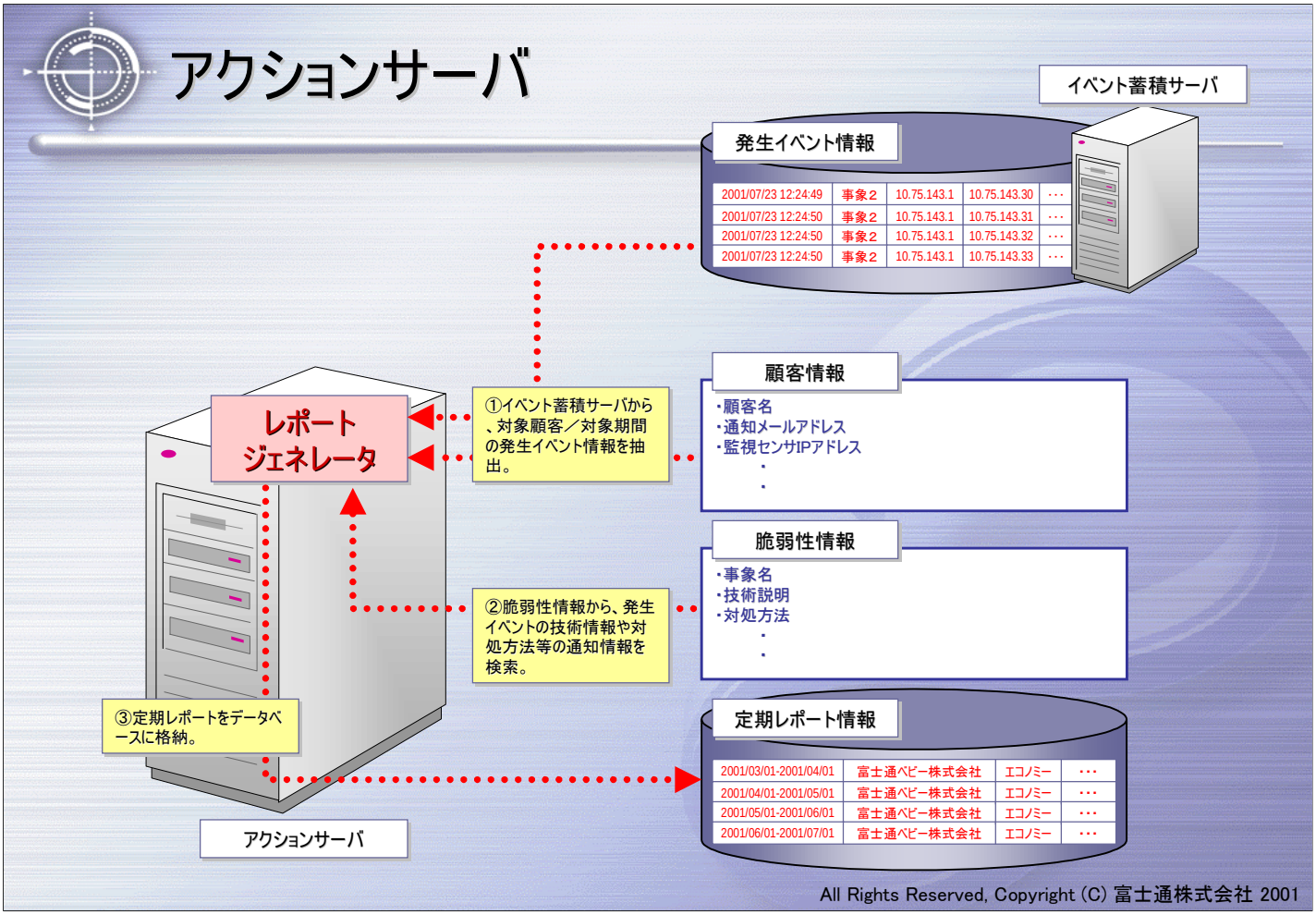


セキュリティ監視サービスエコノミーをご契約いただいたお客様に専用のWebサイトをご提供。

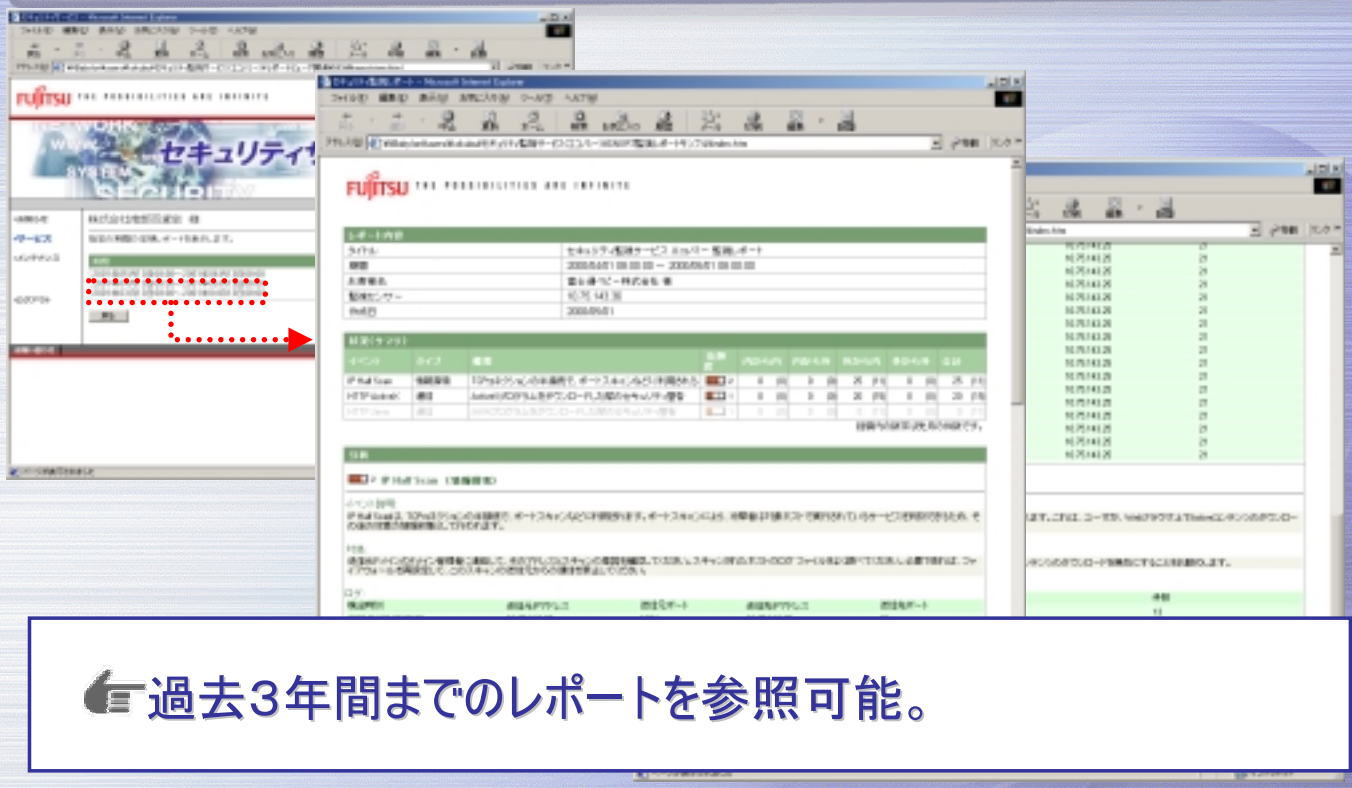
定期レポートご提供に関するシステム的ご説明。

サービス フロー概要



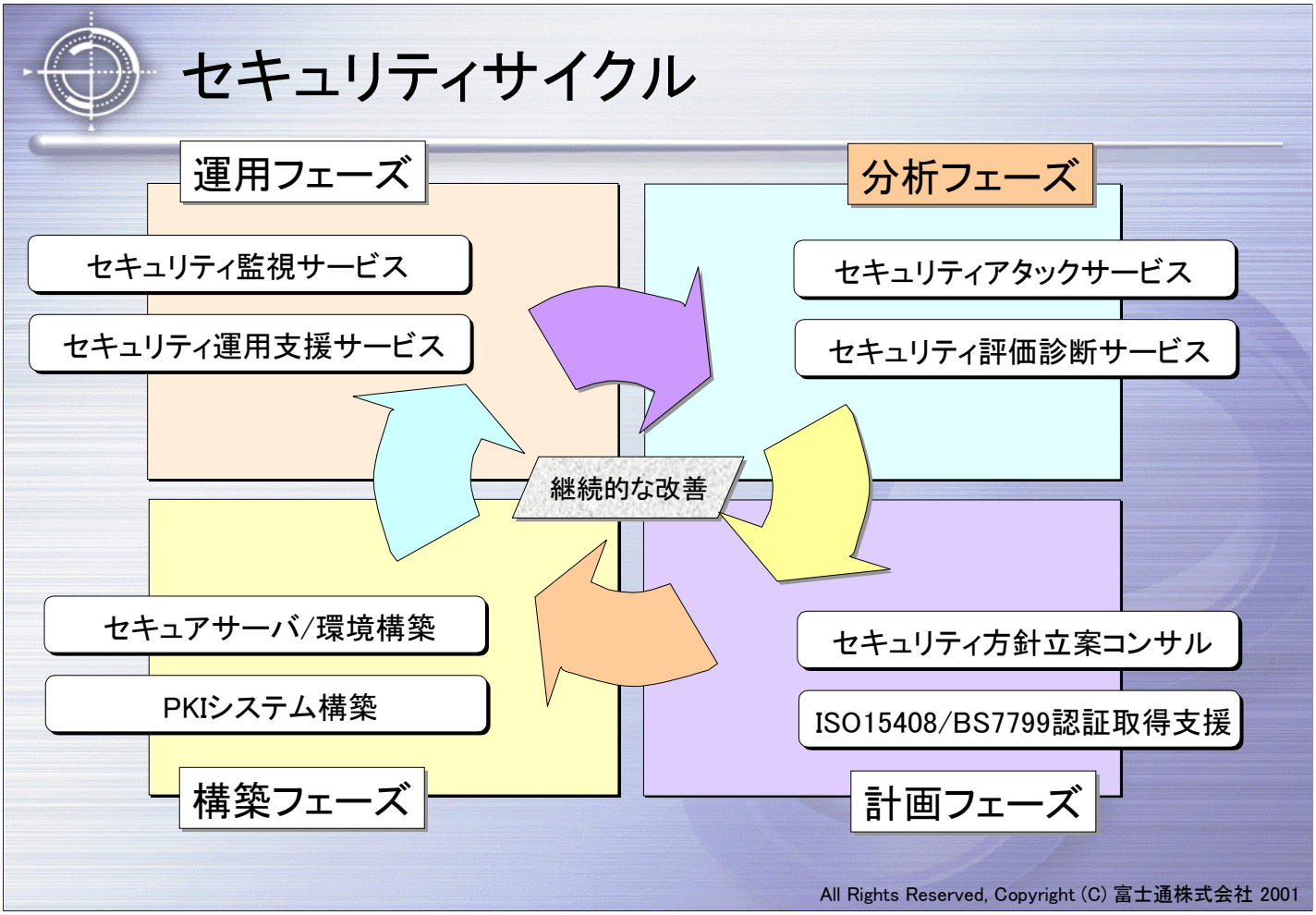


定期レポート参照



過去３年間までのレポートを参照可能。

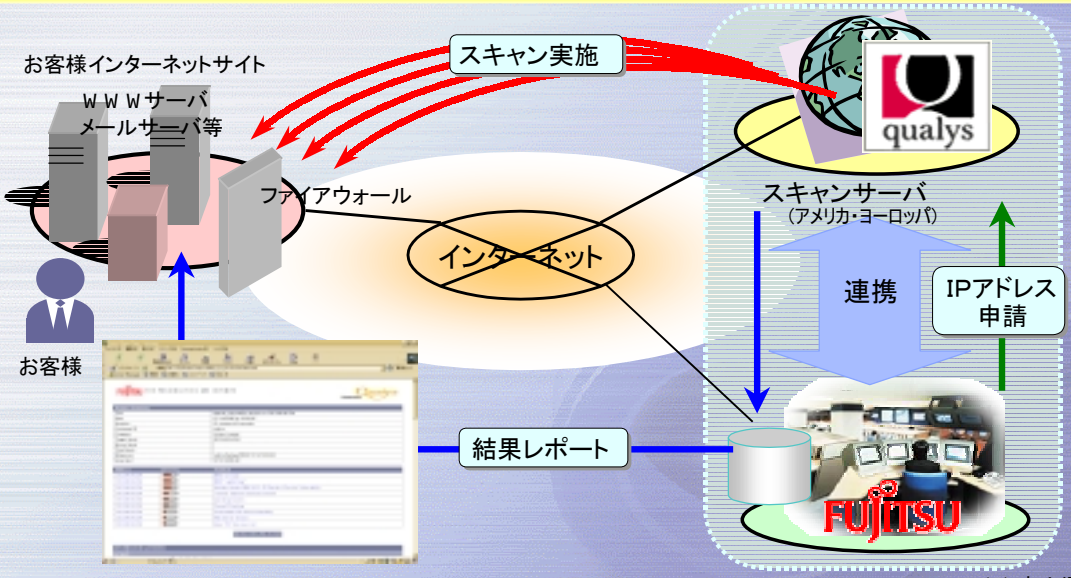
・一ヶ月間のイベント発生状況をご報告。
・過去三年分のレポートを参照することが可能。
・イベントの通信方向ごと（外部→内部、内部→外部、等）に集計。外部からの攻撃ばかりではなく、知らない内に仕込まれた攻撃ツールによって行われる、内部から外部への不正なアクセスを発見することもできる。
・イベントの詳細には、イベントごとに、期間内に発生した全イベントのログも記載される。



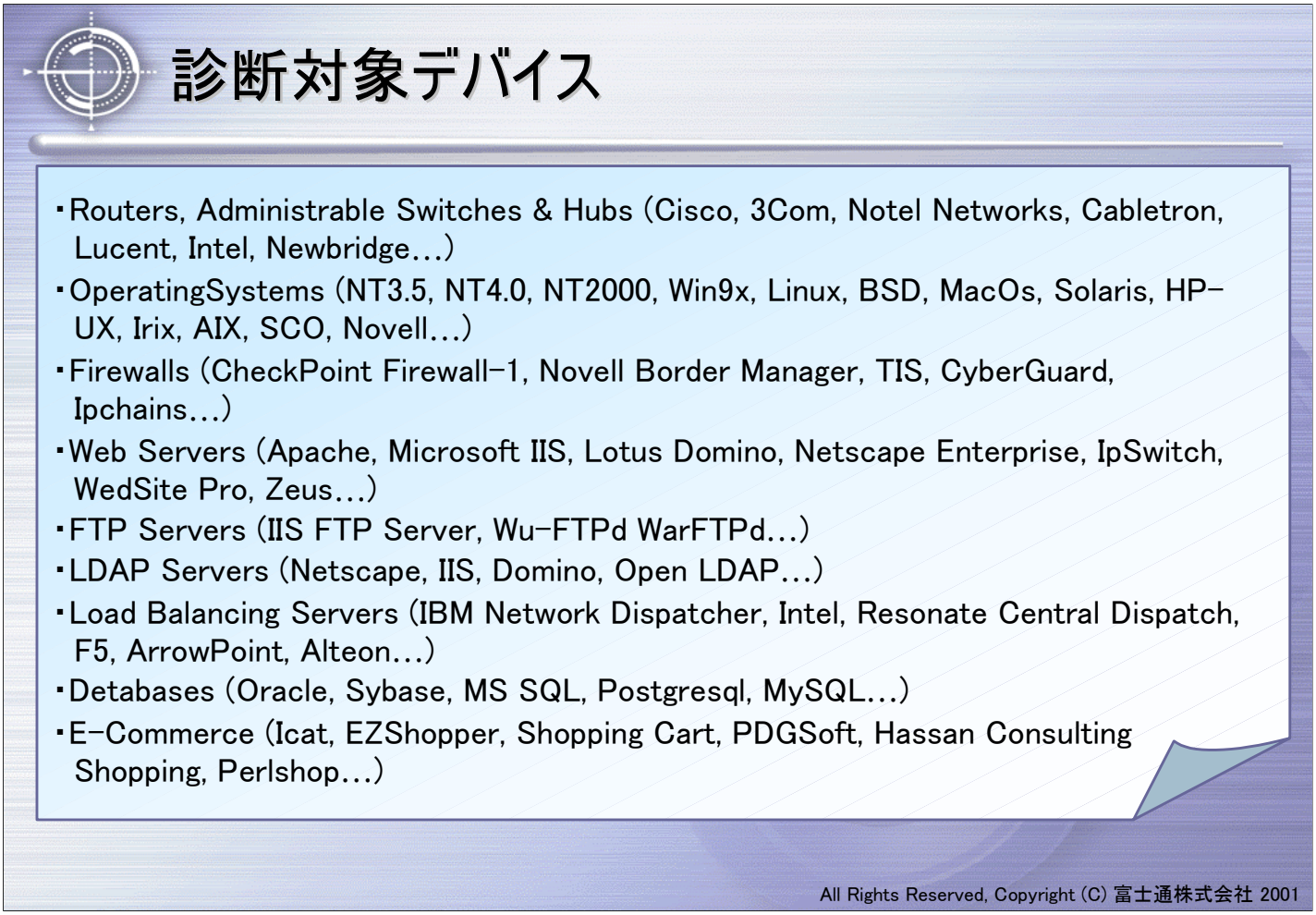
次にセキュリティを維持・継続するサイクルの分析フェーズの中から、セキュリティアタックテストサービスについてご紹介。

アタックテストサービス エクスプレス

- 世界中で高い評価を受けている、米国Qualys社実施の QualysGuard™によるセキュリティアセスメントサービスを、日本国内で初めて提供。
- 迅速なセキュリティホールへの対応。あらたにセキュリティホールが見つかった場合、原則として1日以内に、該当セキュリティホールを検出するアタックパターンが反映される。
- 高速なスキャニング速度 1サーバあたり、(15～20分程度)



アタックテストサービスの中のエクスプレスについてご紹介。
・富士通と米国Qualys社が提携してご提供するサービス。
・ご契約いただいたお客様には専用のWebサイトをご提供。診断結果は、このサイトからご提供。
・新たなセキュリティホールが見つかった場合には、原則一日以内にそのセキュリティホールを検出する診断パターンが提供される。
・契約期間中の診断回数に制限はなし。回数無制限。



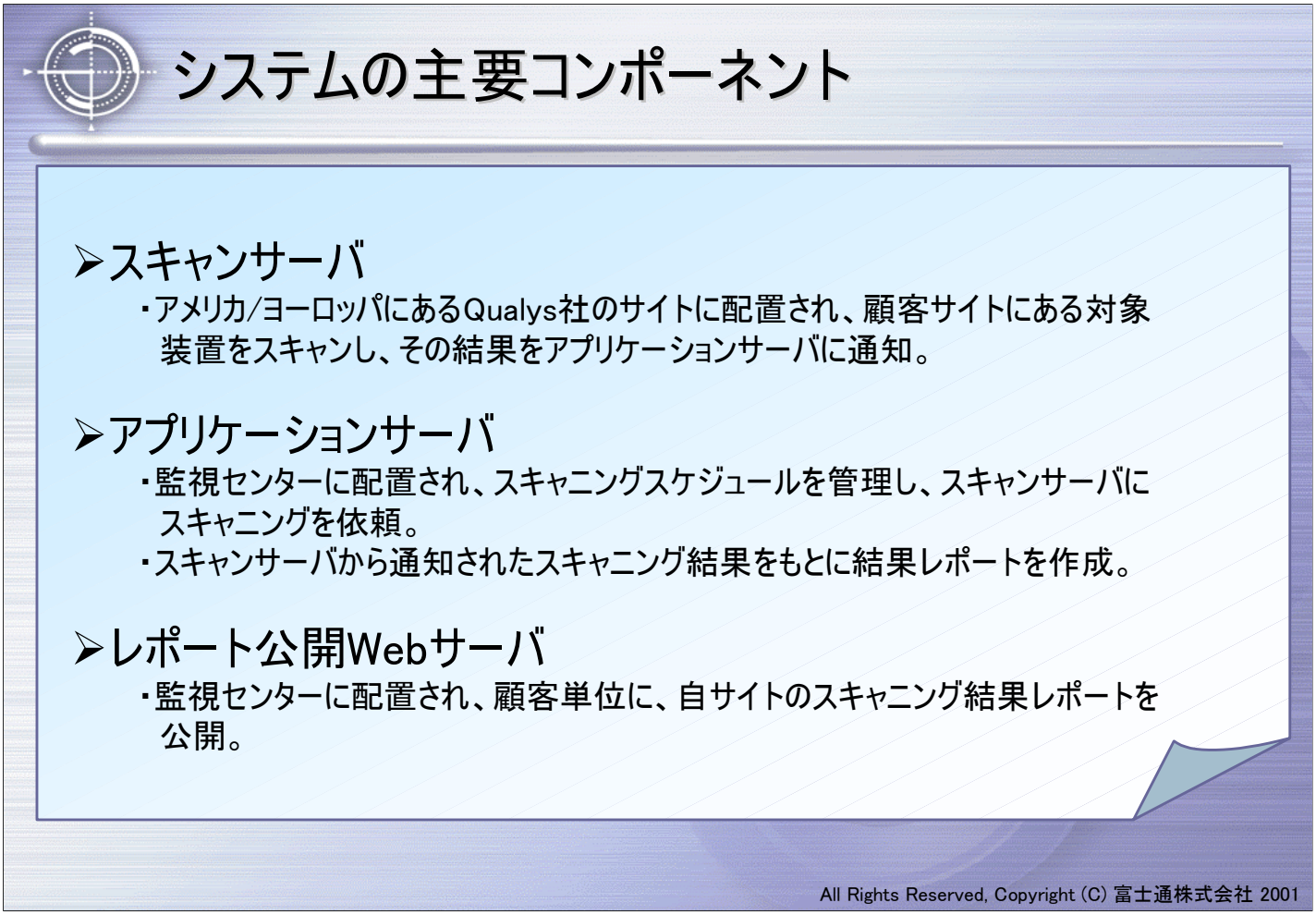
診断の対象となるデバイスは幅広い。

診断項目のカテゴリ

- DNS and Bind
- Back Doors and Trojan Horses
- Brute Force Attack
- CGI
- File Transfer Protocol
- Firewall
- MS FrontPage
- General Remote Services
- Hardware & Network Appliances
- Information Services (NIS, LDAP, WHOIS)
- SNB/Netbios Windows File Sharing
- SMTP and Mail Transfer
- Databases
- E-commerce
- Information gathering
- Mail server
- SNMP
- TCP/IP stasks
- Web server
- MS Windows
- X-Window

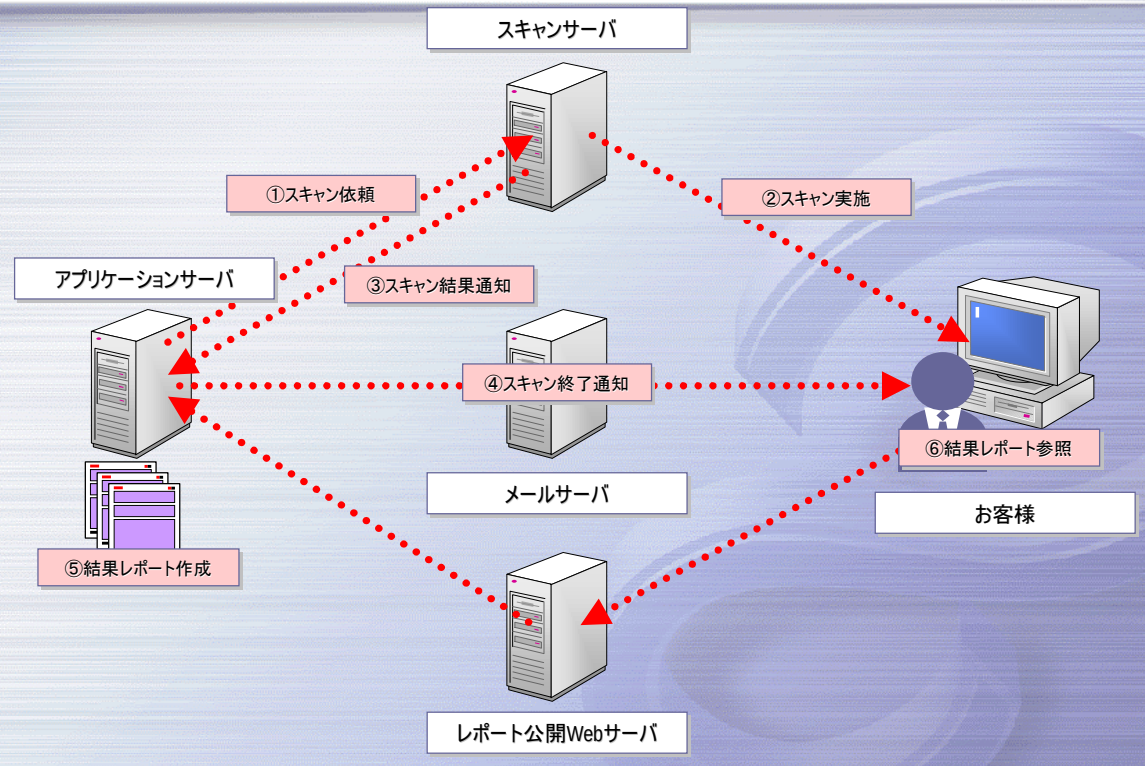
診断は、スキャニングという技術で行う。擬似的に攻撃パケットを送信しないので、日常お使いのまま診断をお受けいただける。診断項目は1000項目以上あり、カテゴリも多岐にわたる。

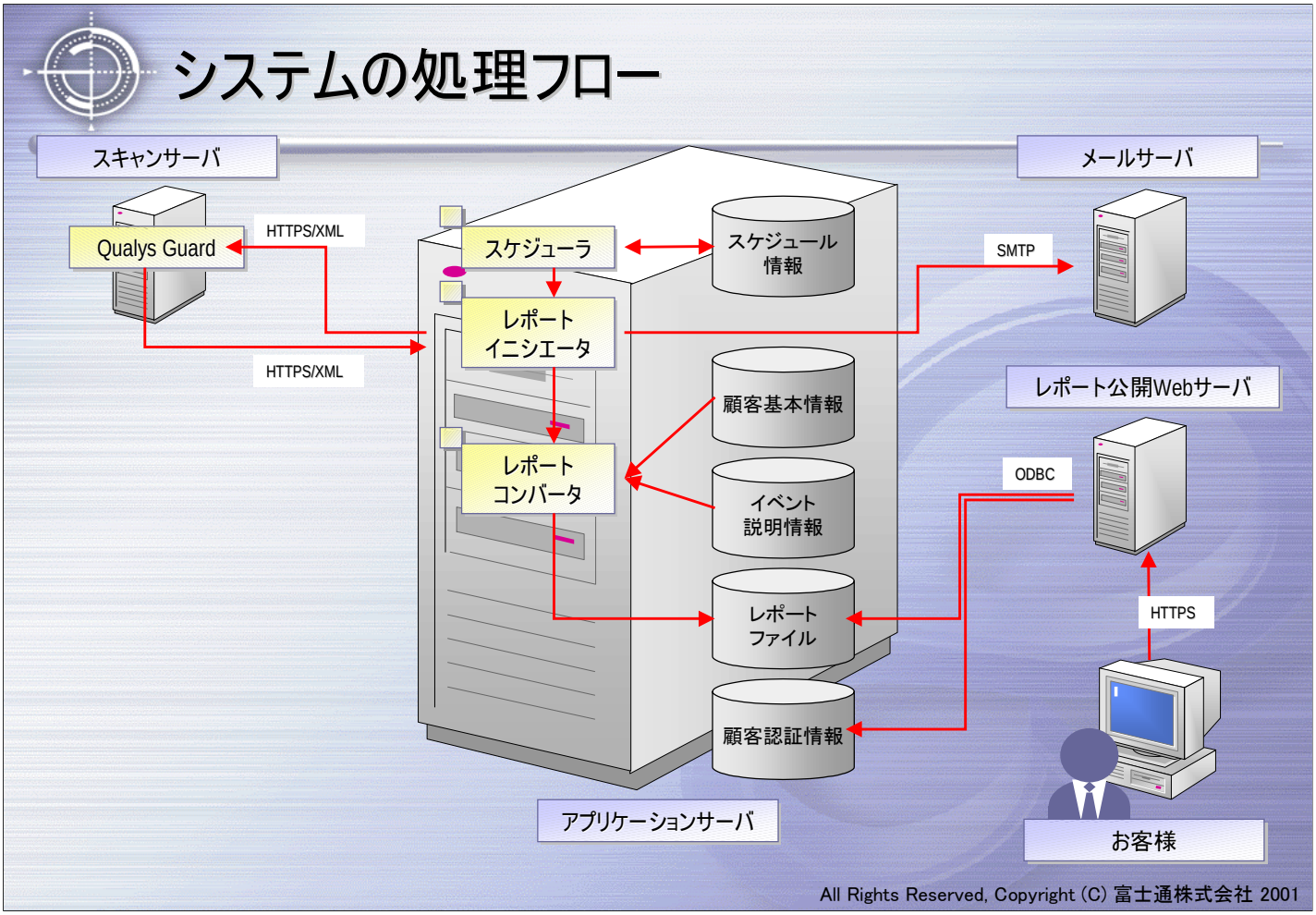
アタックテストサービスエクスプレスのシステムについてご説明。

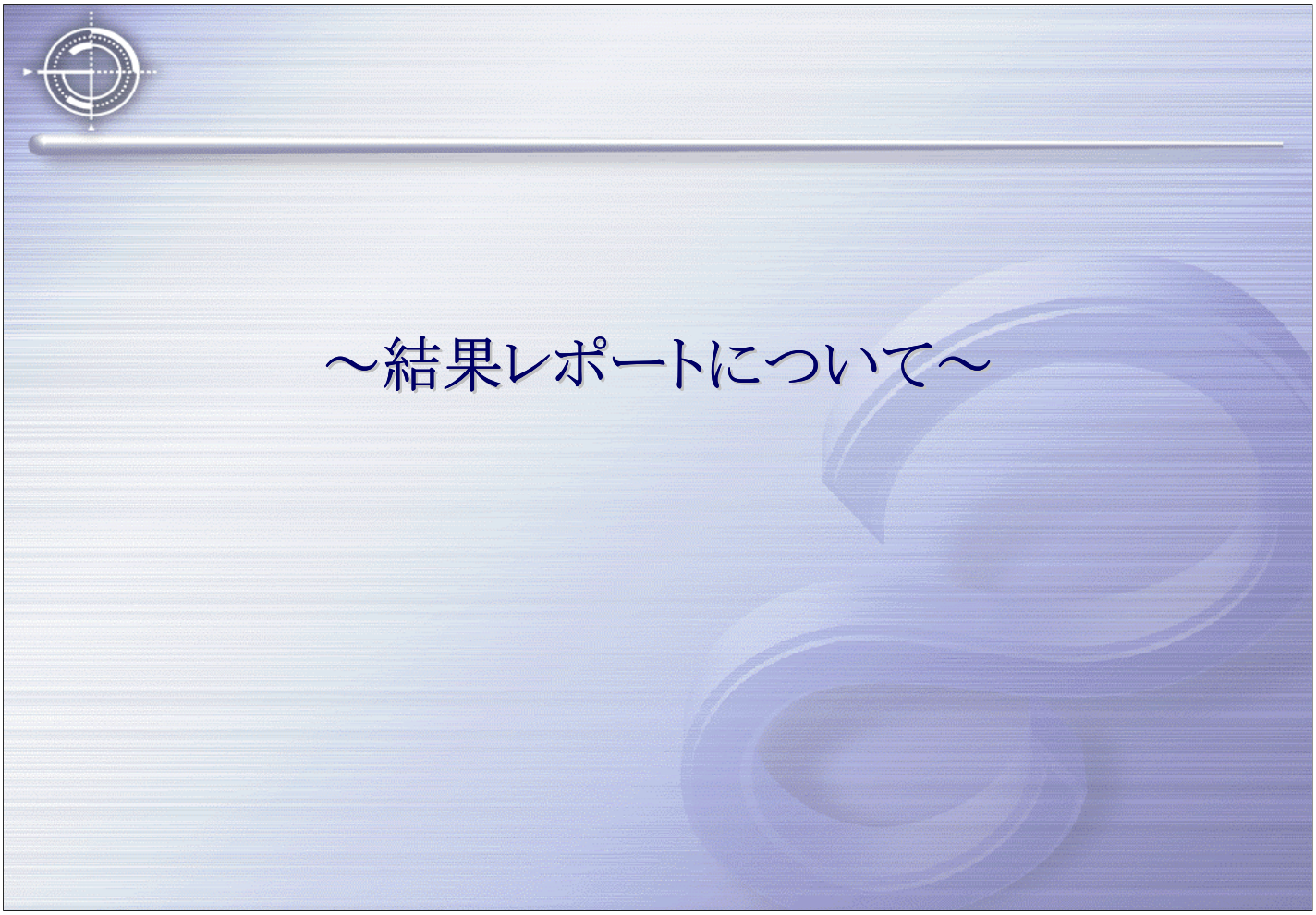


システムの主要なコンポーネントは、
・スキャンサーバ
・アプリケーションサーバ
・レポート公開Webサーバ
の三つ。

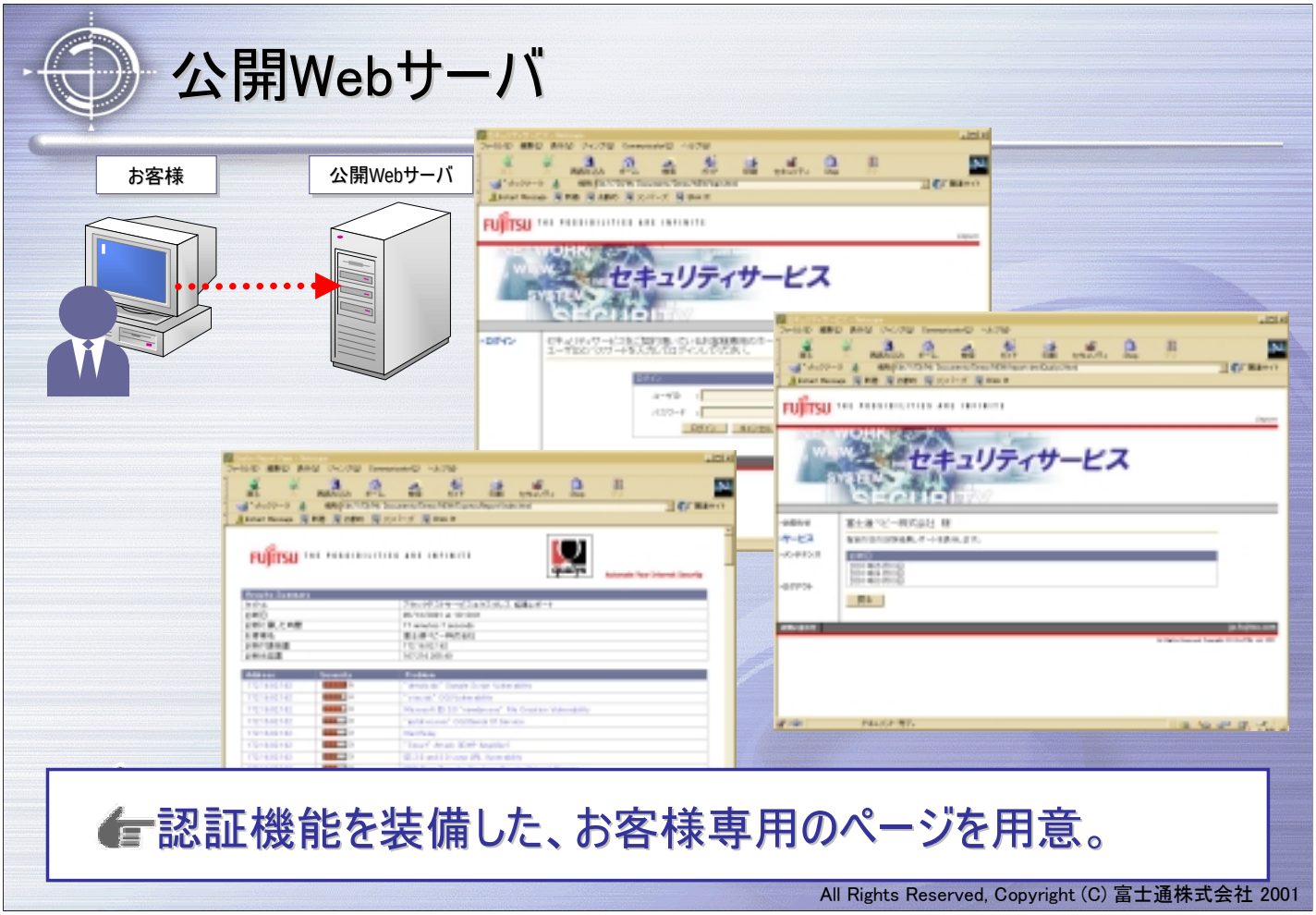
システムの仕組み







結果レポートご提供に関するご説明。



・診断の結果をお客様専用のWebサイトでご報告。
・過去三年分のレポートを参照することが可能。
・レポートは、診断結果だけではなく、その時に行ったスキャニングで取得した情報も併記されるので、
何故、その診断結果に至ったのかがわかり、対処を検討しやすい。
・年内を目処に、レポートの日本語化作業を実施中（順次日本語化コンテンツに変更）。

＜参考＞Qualys社について

・社名：Qualys, Inc.
・本社：1326 Chesapeake Terrace Sunnyvale, CA 94089 – USA
・社歴：1999年セキュリティの専門集団により設立。
本社がSunnyvale（25名）で、リサーチと開発はフランスで実施（合計50数名）。
シリコンバレーのVCであるBessemer Venture Partner と Verisign(証明書発行で有名なセキュリティ会社)からも資金を受ける。
・社長：Philippe F. Courtot
・業務概要：QualysGuard™というソフトウエアツールにより、リモートからセキュリティ監査サービスを提供。この分野での欧米の最先端企業。
セキュリティホールへの対応が早く（一日以内）、ネットワーク負荷を考慮したリモート監査が可能。欧米の数多くの会社（Verisign(US), AKAMAI(US), COLT(U.K) 等）と提携し高い評価を得ている。
MSPアライアンスに加盟。
・ホームページ：www.qualys.com

Qualysの顧客には、UbizenやPredictive Systems等の米国のセキュリティコンサルティング会社や、Apple Computer、Bank of the West、Broadwing等が、名を連ねている。

THE POSSIBILITIES ARE INFINITE

セキュリティサービスに関するお問い合わせ

E-MAIL：secure@ml.sag.fujitsu.co.jp
URL ： http://segroup.fujitsu.com/secure/