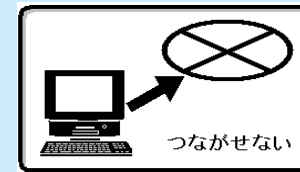
 需要检查的地方太多，成为隐患，需要对应措施。

- 私人电脑带进了公司
- 私自将电脑接入了公司网络
- PC的安全策略的贯彻完全由用户决定

禁止连接



基本篇 对能够接入公司网络的PC进行限制

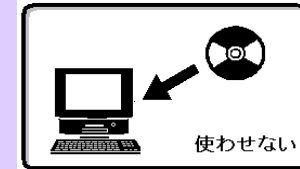
Slide 2

应用篇 贯彻执行接入公司网络的PC的防病毒措施

Slide 3

- PC中安装了与业务无关的软件
- 业务用PC任何人都能登录使用
- 多个人使用了相同的ID和密码
- 基本上没有密码变更

禁止使用



基本篇 禁止安装与业务无关的软件

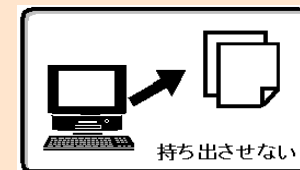
Slide 4

应用篇 定期检查密码

Slide 5

- 重要的信息谁都能访问
- 没有对打印和保存介质的使用进行限制
- 由于害怕信息泄漏，全面禁止将信息拿到公司外部

禁止带出

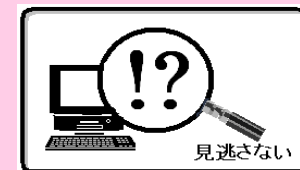


基本篇 对于重要的信息设置访问和带出双重限制

Slide 6

- 设定了访问限制的文件散布在不同地方
- 万一发生了信息泄漏事件，难以找出原因
- 无法防止工作用电脑被用作私人用途

防止疏漏



基本篇 能够追踪下载之后的文件操作情况

Slide 7

应用篇 检查PC的使用情况

Slide 8

- 希望远程解决问题，但是担心安全情况
- 难以把握软件许可协议情况
- 程序更新的工作交给了用户个体
- 无法判断安全情况是否有所改进
- 无法确定管理员的业务

其他用途

远程操作 在连接时通过密码确认对方身份（认证），并给数据传送设置密码

Slide 9

许可协议管理 以可视化的方式对持有的许可协议及其使用情况进行管理

Slide 10

软件分发 自动更新重要程序

Slide 11

掌握安全对策情况 可视化管理安全对策情况，发现无效时迅速采取相应措施

Slide 12



禁止连接

禁止使用

禁止带出

防止疏漏

Q

员工将个人电脑接入了公司网络，但是没有影响吗？！?

员工将个人电脑私自接入公司网络，会给系统带来巨大风险。

未经认证的PC若接入了公司网络，可能导致整个公司系统感染病毒，或者内部重要信息泄漏等重大事件。

A

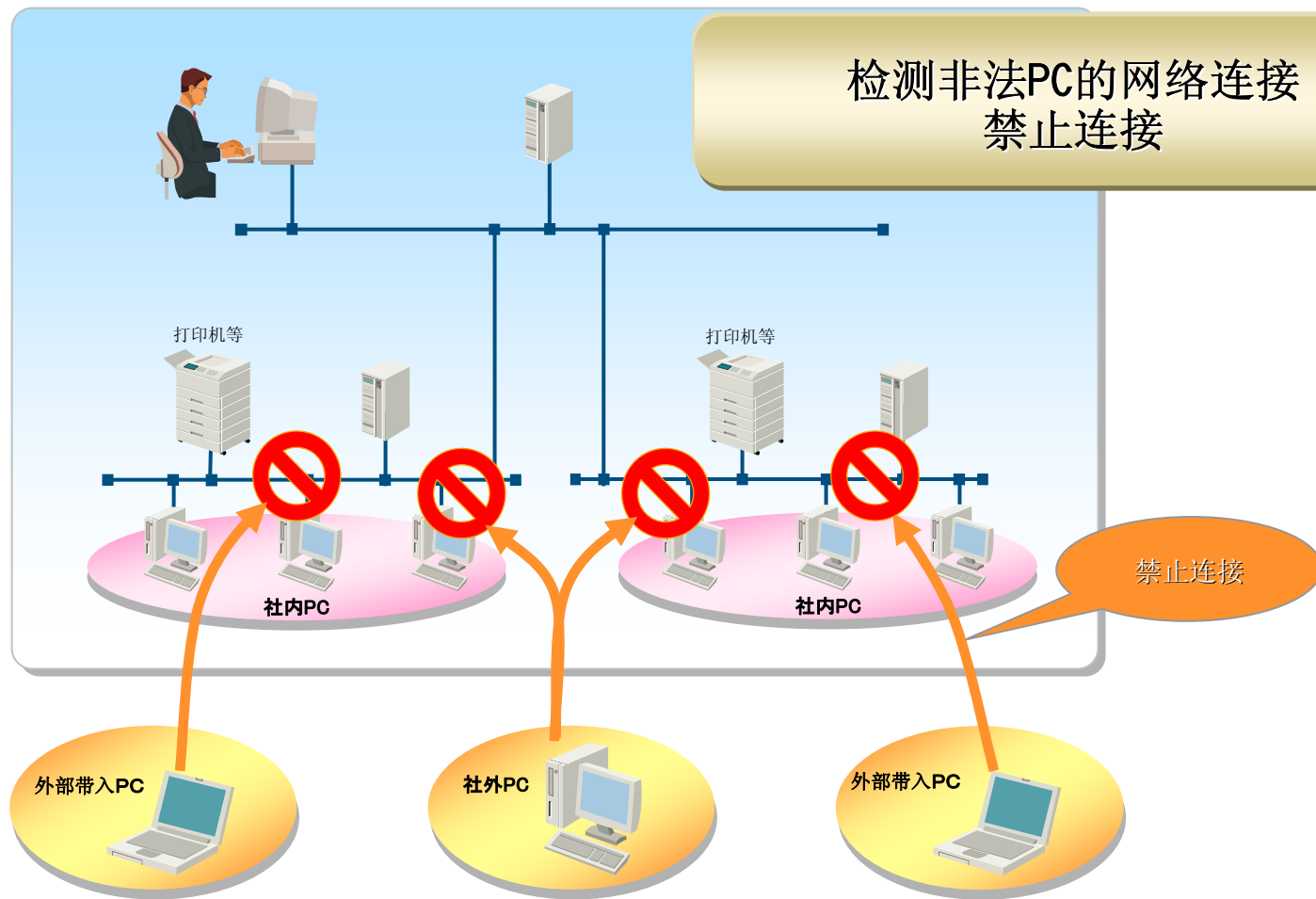
禁止未许可PC的接入

JP1可以实现

禁止未认证PC的网络连接。

通过事先登记可允许接入网络的PC，可以防止未认证PC的非法连接，从而规避感染病毒、信息泄漏的风险。

检测非法PC的网络连接 禁止连接



禁止连接

Point! 管理软件只需要安装在子网内的一台PC上即可。无需变更网络和连接到网络中的PC。

只需三步，简单轻松！

Step 1 监视网络连接

选择“进行网络监视”和“检出非法机器但是不消除（检出和清除不同时执行）”，然后每隔一两周收集一次日志。

No	項目	設定値
1	監視モード	<input checked="" type="radio"/> ネットワークの監視を行う <input type="radio"/> ネットワークの監視を行わない
2	排除モード	<input type="radio"/> 不正機器を検出したら排除する <input checked="" type="radio"/> 不正機器を検出しても排除しない (<input type="radio"/> 検出のみ行う <input checked="" type="radio"/> 検出・排除ともに行わない)

环境设定画面

Step2 注册允许接入网络的PC

网络中连接的所有机器显示在“连接机器”列表中，点选前面的复选框，然后按下“允许连接”按钮，即完成了允许连接机器的登录。

①在“选择”复选框上打“✓”

②按下“允许连接”按钮。

连接机器画面

Step3 禁止未经许可的PC的网络连接

在Step1的设定画面中，选择“检测并清除非法机器”，即完成本步设定。

禁止连接应用篇

禁止使用

禁止带出

防止疏漏

Q

安全策略的贯彻完全由使用者来决定，没问题吗!?

感染病毒的后果不堪设想，将系统安全管理的任务交给使用者是非常危险的。
近年网络病毒扩展的速度越来越快，公司内只要一台电脑感染了病毒，瞬间可能蔓延至整个系统。甚至有由于没有发现自己的机器被感染了而将病毒传染给了商务合作伙伴的事例。

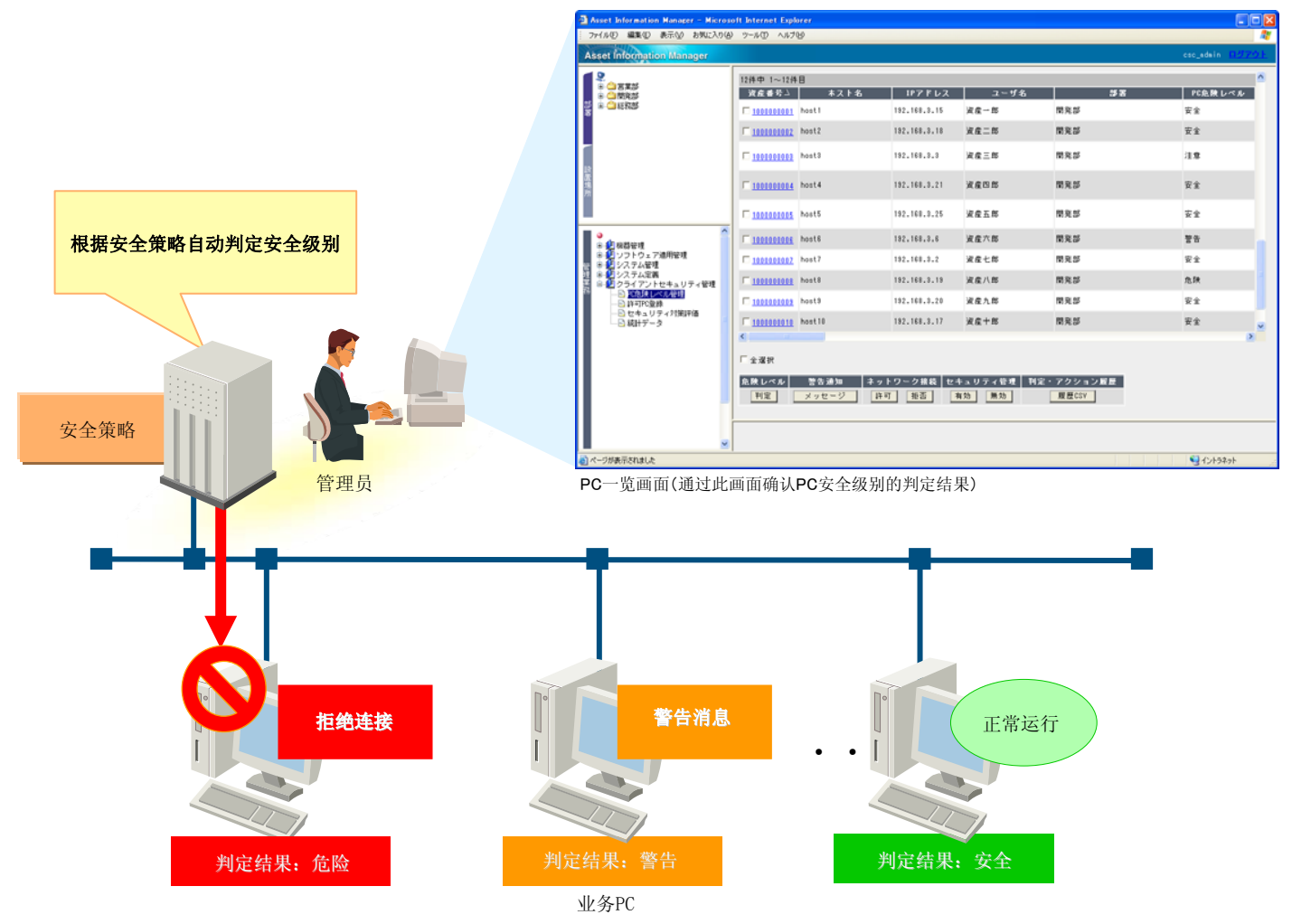
A

查找并隔离中毒电脑

JP1可以实现

自动检测PC的安全级别，强制隔离

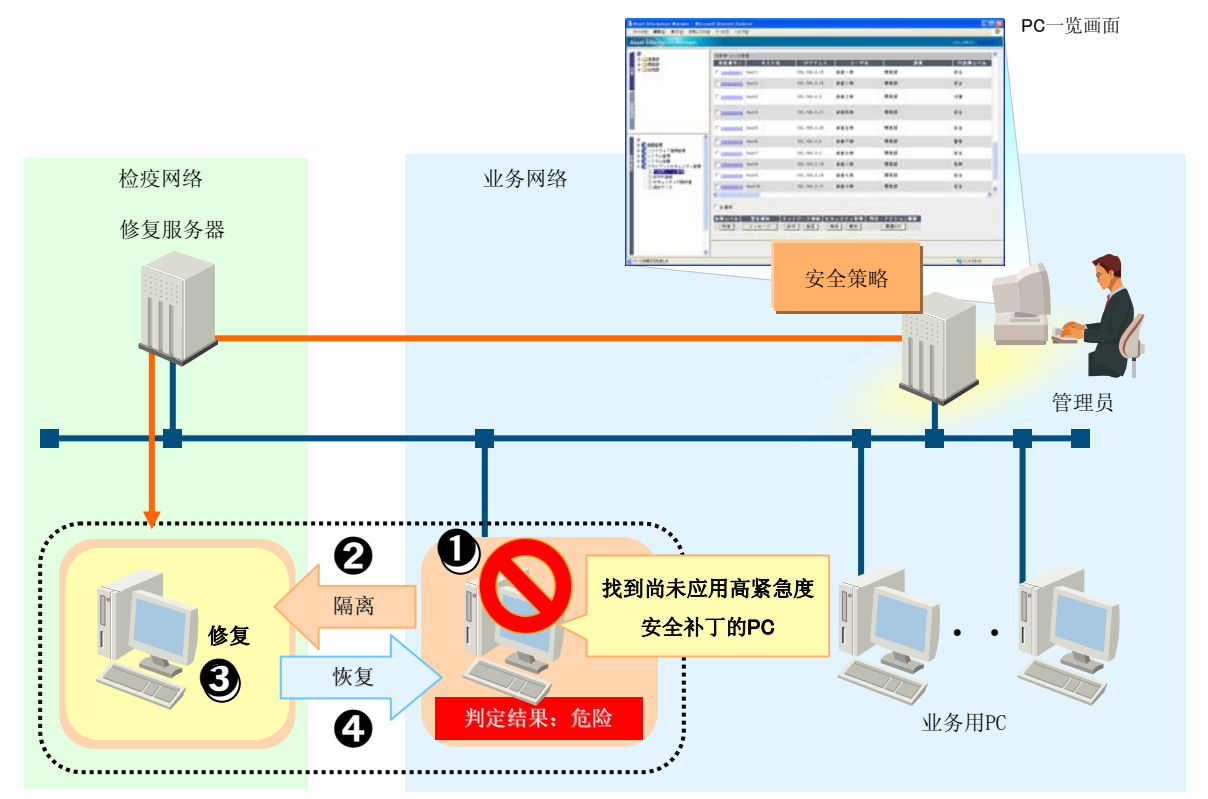
能够对连接到网络中的PC的安全情况进行自动判定，将判定为危险的PC从网络中隔离出来。
确保企业内部网络不受病毒侵扰。



Point! 可以给不同部门设定不同的安全策略。
防病毒软件的最新定义文件、安全补丁信息等都可以自动反映到安全策略中。

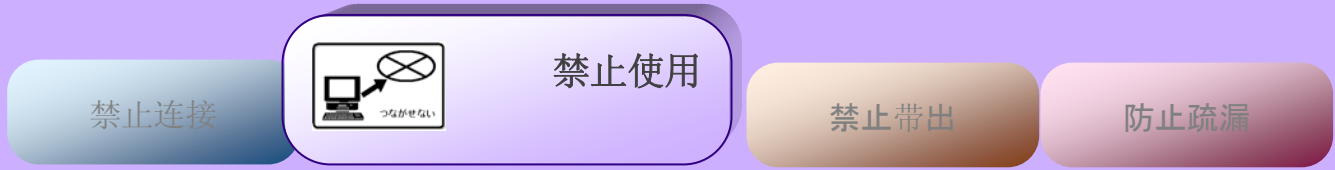
以下功能也能实现

对安全对策不完善的电脑自动进行修复。
自动修复从网络中被隔离出来的存在安全漏洞的电脑，修复完成后恢复网络连接，从而确保网络环境始终安全。



- ① 连接到公司网络。
违反了安全策略的PC被从公司网络中隔离出来。
⇒ 这时违反了安全策略的PC上将显示对策指示消息。
- ② 连接到修复服务器。
- ③ 自动安装高紧急度的安全补丁。
⇒ 安装后，重新判定安全策略。
- ④ 判定为安全后，重新连接到公司网络。

【什么是安全策略?】
为了维护信息安全所制定的一系列必须采取的措施或必须遵循的规则。



Q 公司系统中是否安装了与业务无关的软件?

未经许可的软件被安装，也会给企业系统带来风险！
软件可能存在安全方面的漏洞，如果不加筛选的安装过多软件，可能存在系统崩溃、信息泄漏等隐患。

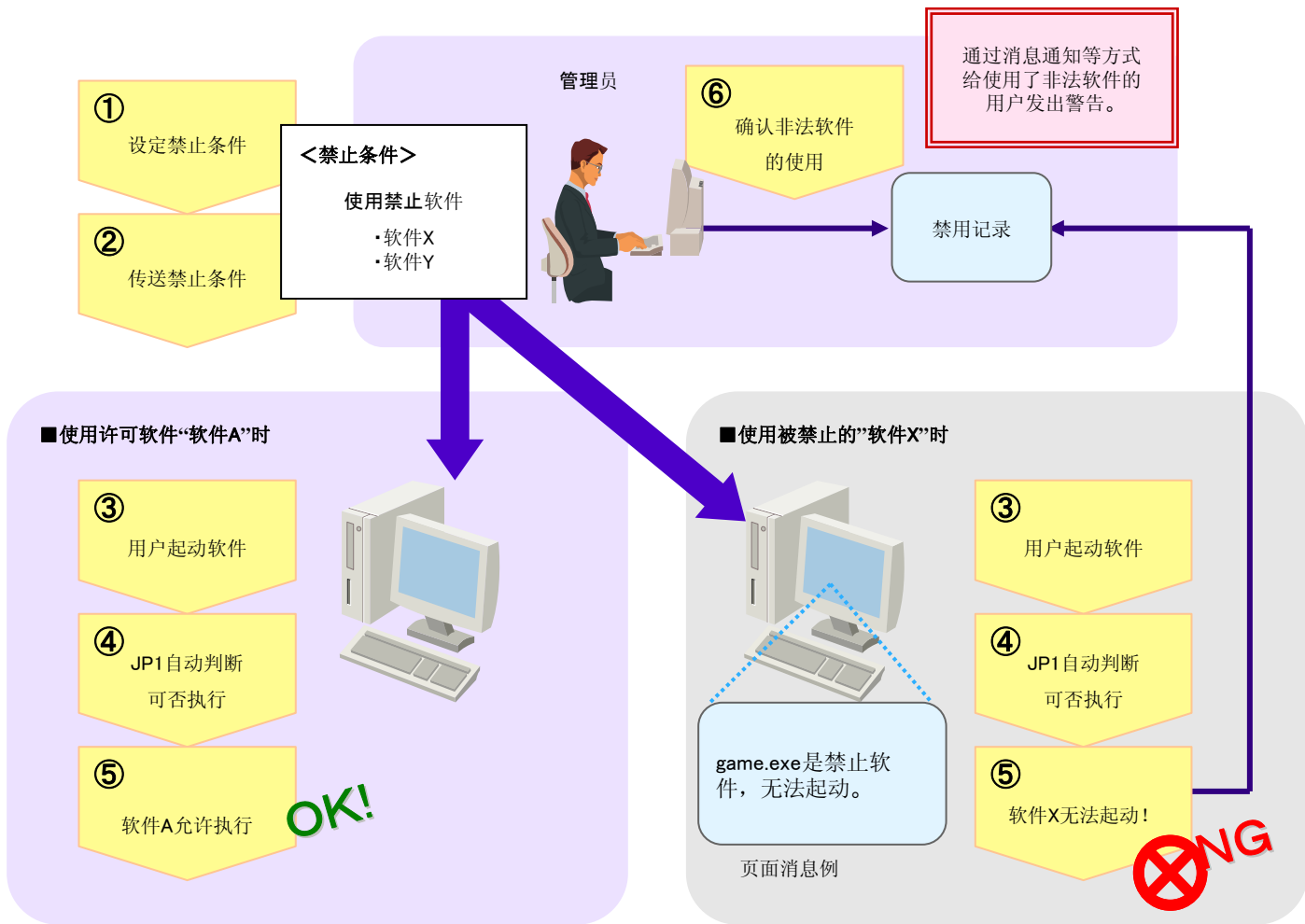
A

禁止启动未许可软件。

JP1可以实现

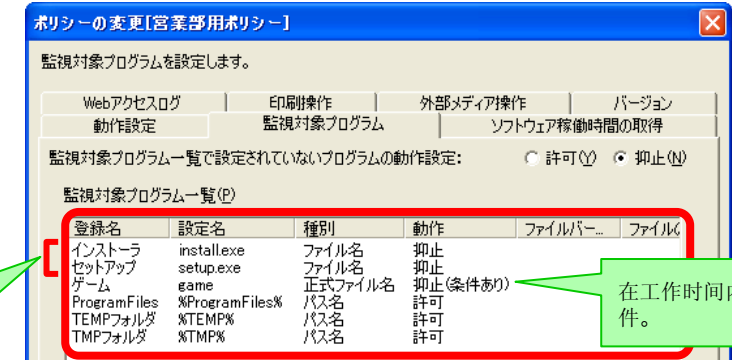
禁止启动未经许可的软件！

即使制定了公司制度，仍然可能会有些用户在不知道风险的情况下，出于兴趣背着管理员安装一些与工作无关的软件。JP1可以禁止此类软件的启动，并且把握这些软件的使用情况，给用户发出相应警告。



通过简单的屏幕操作，实现细致的控制功能

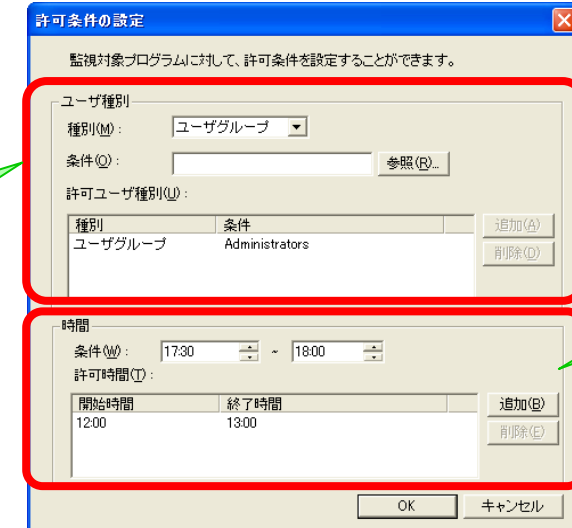
指定禁止软件名称



对于随意安装、或者不更改系统配置的绿色安装和设置，JP1都能够进行禁用或控制。

在工作时间内禁止启动游戏软件。

指定允许的用户和时间



指定允许使用的用户或用户组

指定允许启动的时间段

指定时间段的许可方式也非常有效。

JP1可对系统中软件可使用的时间段进行控制。

- 【例1】**特定的业务系统仅可在 8:00~18:00 之间执行
→通过限制非工作时间段中业务系统的执行，能够减小重要系统的非法访问及数据泄漏风险。
- 【例2】**仅允许在午休时(12:00~13:00)启动OS自带的游戏程序。
→如果全面禁止可能遭到员工抵触，通过此方式可以避免。



Point! 能够设定禁止使用的软件或者允许使用的软件。
根据需要，可将两个条件组合使用。

- 禁止连接
- 禁止使用应用篇
- 禁止带出
- 防止疏漏

Q 业务用PC设定的密码可能被破解 !?

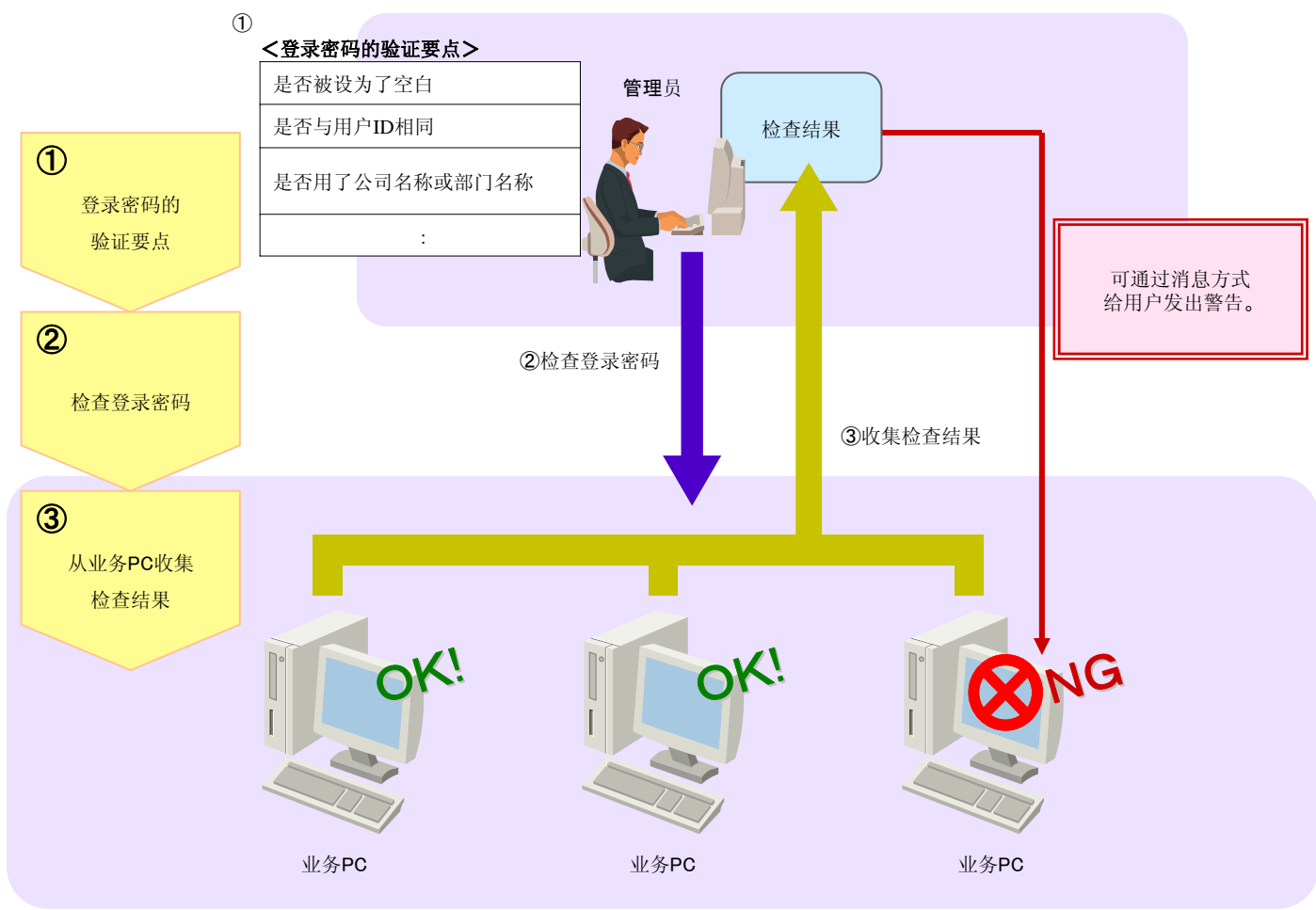
A 禁止使用易被破解的密码

马虎大意的密码设定，存在很大的风险！
随着IT系统越来越广泛的运用，需要设定密码的情况也越来越多。但是，是否有的密码被设为了空白或者非常简易的字符串呢？这种情况就存在PC的密码被人破解并恶意使用的可能性。通过网络的非法访问、信息盗用、以及病毒传播的事件也时有发生。

JP1可以实现

检查当前的密码是否能够被其他人破解！

举例来说，哪怕只有一台电脑的Windows登录密码被人破解，那么整个系统都会有被非法访问的危险。JP1可检测多台PC的Windows登录密码是否被设为了空密码或者容易被人破解的密码。



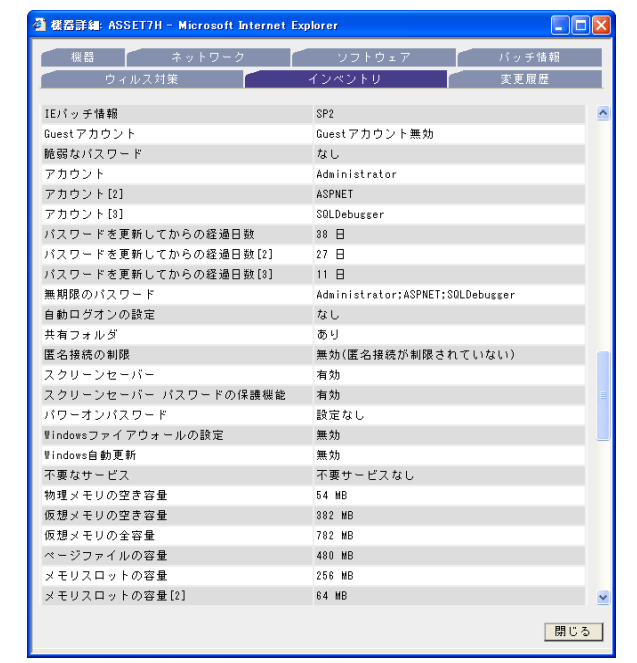
还能实现以下功能

除此之外，还能查看以下信息

要保证系统的安全，首先要了解系统现状。以下这些设定在信息安全的角度上属于“危险”情况。JP1可从这些角度对系统进行全面检查，从而减少PC被他人恶意使用的风险。

JP1可检查的“危险设定”的例子

- 密码**
 - 密码是否为空
 - 是否设定了容易推测的密码
 - 是否设定了没有期限的密码
 - 自从上次更新已经过了很长时间，等
- 屏保**
 - 没有设定屏保
 - 没有设置屏保密码，等
- Windows的设定**
 - 设定了自动登录
 - 自动更新被设为无效，等
- 无意的或者不适当的设定**
 - 使用有共享文件夹
 - Guest账号有效
 - 存在不需要的服务
 - 未对匿名连接进行限制，等



机器详细画面

Point! 可根据需要添加密码的验证要点。
例：密码中是否包含了公司名、部门名或者项目名。
通过自行添加各种公司内部可能存在的密码，能够更强有力的保护系统的密码安全。

密码是既方便又有效的安全措施。

很多人会觉得密码设定是一件很麻烦的事情，然而密码管理功能未被充分利用是非常可惜的。

充分合理的运用密码，是信息安全管理中最基本、最简单、也是最有效的方式。反之，如果对密码的设定掉以轻心，可能给整个系统带来不可想象的严重后果。通常，在设定密码时，最好设定一个长度下限，并且规定必须同时包含英文字母和数字。同时，密码还必须定时更换。



Compliance Memo



Q 重要信息是否在不为人知的情况下被带出了公司?

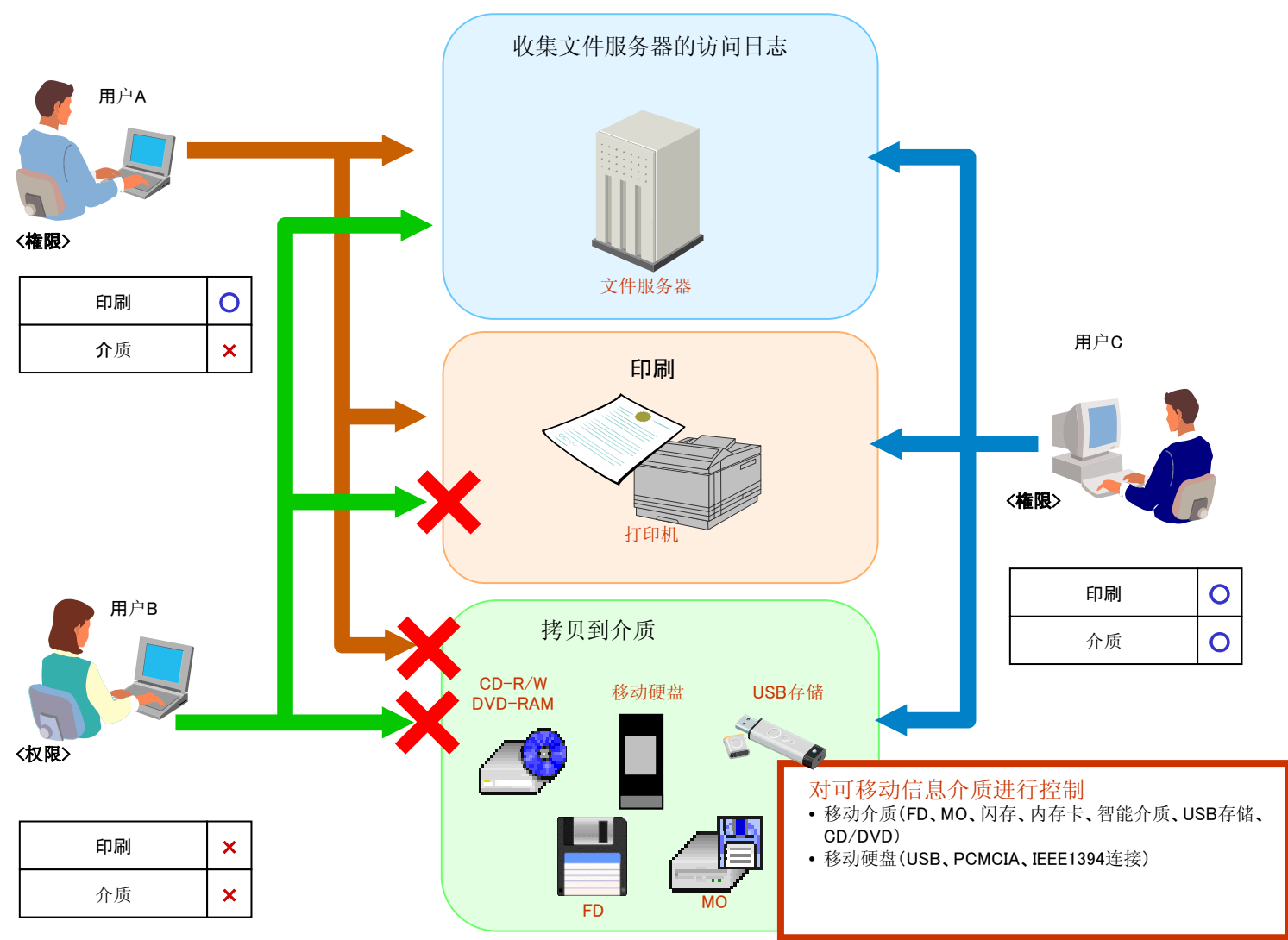
A 对于重要信息
设置浏览和带出双重保
护

信息泄漏是企业经营的大患！
如果系统没有一个严格控制信息带出的机制，那么信息泄漏事件的发生也就不难以想象了。
倘若其中包含了重要的顾客信息，除了经济赔偿之外，还可能导致企业信誉的丧失。

JP1可以实现

只允许有权限的人将信息带到公司外

可针对不同部门和员工，设定不同的信息浏览、更新、打印、拷贝等各种权限。没有权限的员工将无法把信息带出公司。



Point! 没有浏览权限的用户或者部门无法查看这些信息。
即使有浏览权限，也无法将其带出公司。

信息泄漏的渠道多种多样

根据调查数据，信息泄漏有“书面”、“Web或网络”、以及“FD等存储介质”等多种渠道。其中，由于电子媒体导致的信息泄漏事件逐年递增，同时，印刷品导致的信息泄漏事件也完全没有减少的迹象。

- 重要的数据是否能够轻易通过打印机打印出来？
 - 同样的数据，对打印出来后的印刷物的处理是否过于草率？
- 非必要的情况下不打印数据，这是防止信息泄漏的第一步。

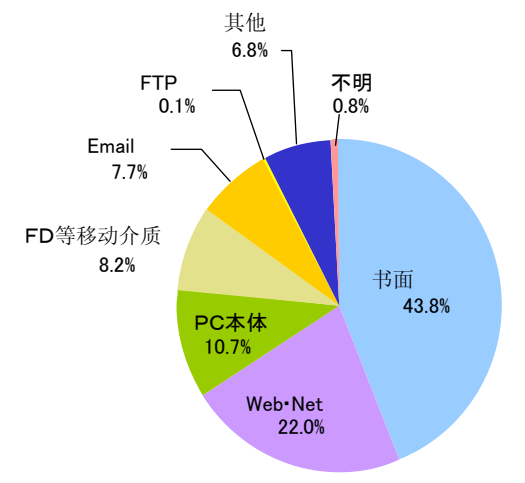


图1 信息泄漏不同渠道的比例

由电子数据导致的信息泄漏事件规模庞大！

从件数上来看，书面介质导致的信息泄漏事件占到43.8%（图1），但是从受害群来看，比起书面介质，由“Web或网络”、“FD等移动介质”导致的电子数据的流失危害更大（图2）。USB存储等移动介质，能够保存的电子数据容量庞大，因此，哪怕只发生了一次信息泄漏，其泄漏的数据量可能要远远大于书面信息的泄漏，而由此引起的经济赔偿等损失也势必更加严重。

- 是否把业务相关数据保存到电子介质上，然后带回家里工作？
 - 由于携带非常方便，丢失后可能不能马上发现？
- 非常方便的电子存储介质才更需要严格的保护手段。

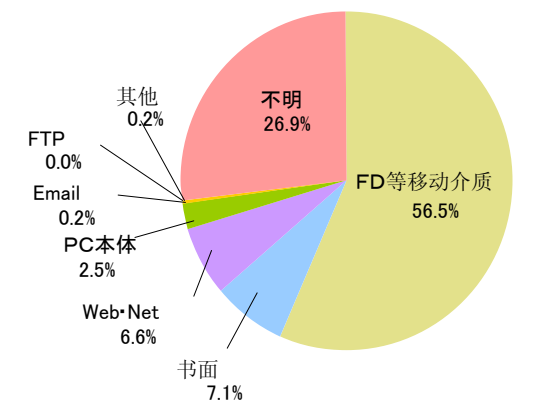


图2 不同渠道信息泄漏事件的受害群比例

出自：NPO日本网络安全协会
2006年信息安全事件相关调查报告书



防止疏漏

禁止连接

禁止使用

禁止带出

Q

重要的信息或许被私自拷贝到个人电脑上了 !?

哪怕是仅仅出于“参考”目的拷贝的信息，也可能成为重大信息泄露事件的导火索。

对于原本应该谨慎管理的重要业务信息，有时可能会出于“仅供参考”或者“给其他资料提供话题”等随意的目的被拷贝到个人电脑上。

A

可追踪到 重要数据的拷贝操作

JP1可以实现

可视化追踪文件操作，杜绝信息泄漏！

JP1可对指定的文件的操作记录进行追踪，能够通过GUI确认其“从哪被拷贝/移动”“拷贝/移动到哪”。

即使中途文件名称被更改也没关系。这样，即使发生了业务信息泄露的事件，也能通过文件追踪功能找出原因。同时，向公司内部宣布此功能的应用，能够大大抑制这种非法操作的发生。

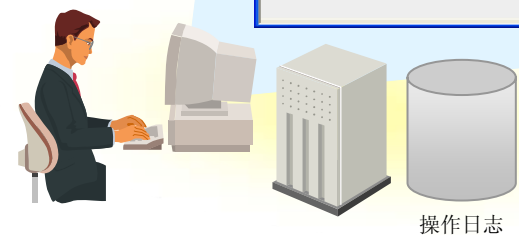
文件操作追踪页面

操作日志一览表

以选中的文件为起点，能够追踪其前后的操作轨迹。

日時	種別	ファイル名	操作先
2008/02/13 22:45:32	コピー	社員名簿.xls	デスクトップ
2008/02/13 22:45:51	開く	社員名簿.xls	デスクトップ
2008/02/13 22:45:52	プログラム起動	社員名簿.xls	デスクトップ
2008/02/13 22:45:52	プログラム起動	社員名簿.xls	デスクトップ
2008/02/13 22:45:52	プログラム起動	社員名簿.xls	デスクトップ
2008/02/13 22:45:53	プログラム起動	社員名簿.xls	デスクトップ
2008/02/13 22:45:56	プログラム起動	社員名簿.xls	デスクトップ
2008/02/13 22:45:56	開く	社員名簿.xls	デスクトップ
2008/02/13 22:46:10	コピー	社員名簿.xls	デスクトップ
2008/02/13 22:46:14	コピー	社員名簿.xls	デスクトップ
2008/02/13 22:46:22	削除	社員名簿.xls	デスクトップ
2008/02/13 22:46:22	削除	社員名簿.xls	デスクトップ
2008/02/13 22:46:22	削除	社員名簿.xls	デスクトップ
2008/02/13 22:46:29	コピー	社員名簿.xls	デスクトップ
2008/02/13 22:46:40	名称変更・移動	社員名簿.xls	デスクトップ
2008/02/13 22:46:43	削除	社員名簿.xls	デスクトップ
2008/02/13 22:46:58	プログラム起動	社員名簿.xls	デスクトップ
2008/02/13 22:47:00	プログラム起動	社員名簿.xls	デスクトップ

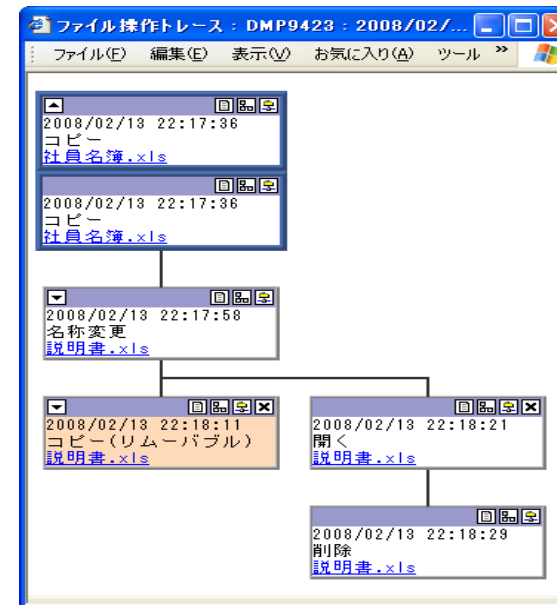
操作日志



可在操作日志一览页面中选择想要调查的操作。

对各种文件操作都能以可视化的方式进行追踪。

一个操作显示为一个 [操作图标]。JP1能够识别的操作如下。



1. 将“员工名单.xls”文件从文件服务器*1拷贝到了桌面
⇒ 还能确认拷贝前后的文件名。
2. 将“员工名单.xls”文件名改为了“说明书.xls”
⇒ 可确认更改后的名称。
本例中，“员工名单.xls”被更为了“说明书.xls”。
3. 将“说明书.xls”文件拷贝到了移动介质中
⇒ 将桌面上的该文件拷贝到了移动介质中。
4. 在桌面*1上打开了“说明书.xls”文件
⇒ 可对拷贝源的文件操作进行追踪。
在此例中，可以看到桌面上的该文件被打开。
5. 从桌面*1上删除了“说明书.xls”文件
⇒ 在桌面上删除了拷贝源的文件

注※1 以上画面是仅有文件名的“概要显示”页面，切换到详细显示页面，既可查到该文件被从哪拷贝到了哪。
注※2 将文件拷贝到外部介质的操作会用不同颜色显示出来。

在万一发生的紧急情况下是否能迅速做出处理是关键

对文件操作进行记录和追踪，是不是意味着公司对员工持不信任态度呢？这是一种误解。

为了证明系统的日常运行管理得到了正确的贯彻执行，在发生万一不备的情况下，若要迅速找到原因，确定影响范围，并及早做出对应以保护公司和员工，这种对文件的追踪体制就非常必要了。

遗憾的是，100%完备的信息安全对策是不太现实的。但是，JP1可以做到近似于100%的管理，亦即在万一发生信息泄露事件的情况下，通过迅速有效的处理，将影响范围降至最低。



Point! 除了文件拷贝外，还能对文件删除、移动、更名、新建、以及打开文件等操作进行追踪。



防止疏漏
应用篇

つなげない

禁止使用

禁止带出

Q

业务用PC是否被用作了工作之外的用途 !?

出于私人目的使用公司电脑也存在安全隐患!

日常用惯了的公司电脑,可能出于方便被用作了私人用途。而出于非工作原因使用业务PC,不仅加速了公司资产的损耗,还有可能引起安全方面的问题。

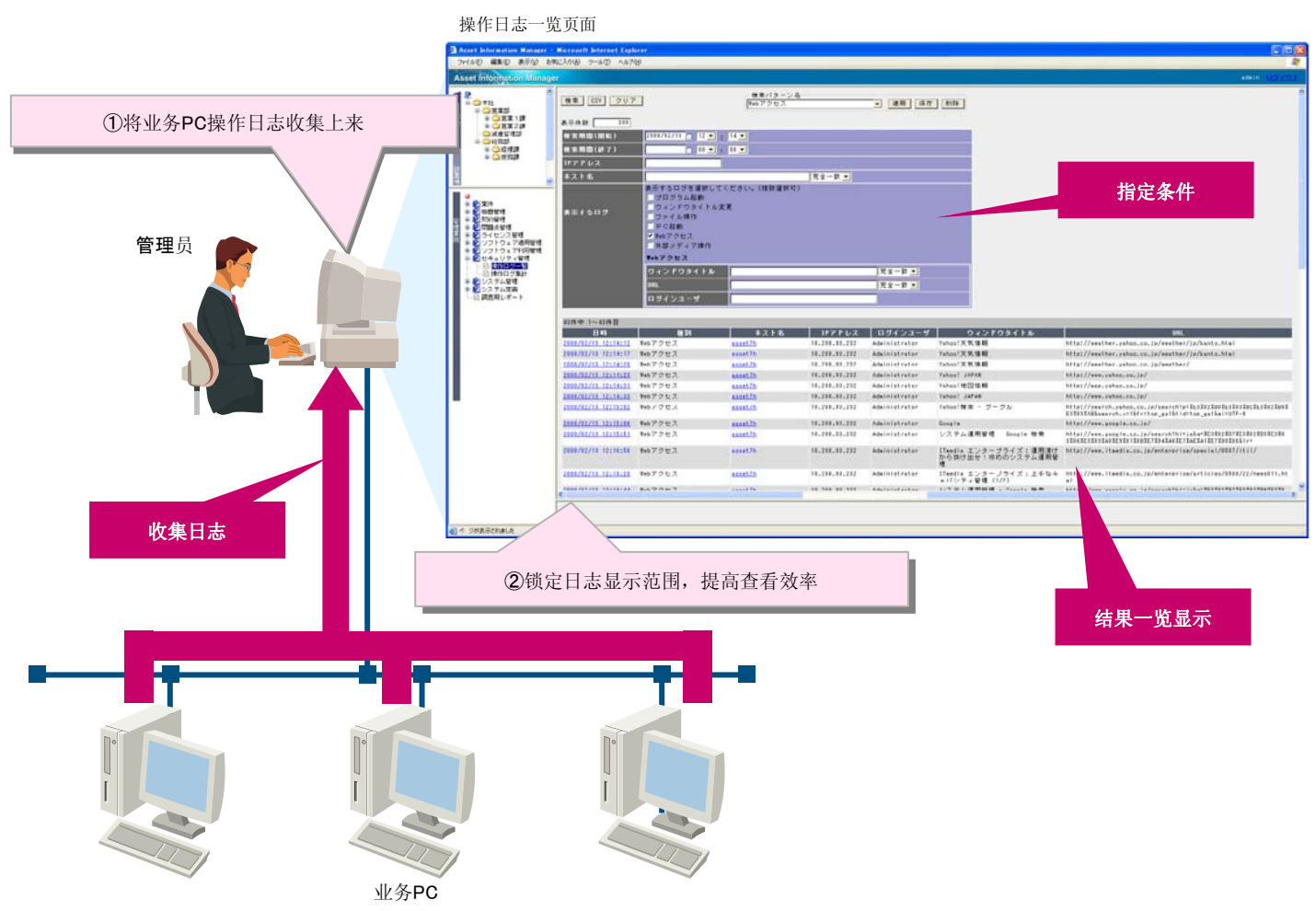
A

防止业务PC不当使用

JP1可以实现

检查PC的使用情况

管理员可通过JP1了解用户的PC使用情况和操作情况,不仅能够发现被禁止的操作,还能看到每种工作花费了多长时间。同时,如果事先将此监测功能公布给员工,还能起到抑制不当操作的作用。



Point! · 从PC启动到结束,几乎所有操作都能以日志的方式被记录并收集。
· 也可以只收集跟特定操作相关的日志。

可查看的操作内容

~从日志可以看到员工A的一天~

以下左侧是从员工A使用的PC收集上来的日志。右侧是从该日志了解到的员工A的操作记录。由此,万一发生安全事故时,可以查找到产生了影响的操作,并为迅速找出原因做出贡献。

<收集到的日志>

- 9:00**
启动PC。
登录Windows。
- 9:30**
启动邮件系统。
打开收件箱。
- 10:00**
启动Microsoft Powerpoint。
新建文件“会议资料.ppt”。
启动Microsoft Excel。
打开文件“调查统计结果.xls”。
- 12:00**
启动Microsoft Internet Explorer。
打开http://www.***** (URL)。
- 15:00**
打印“会议资料”。
- 16:00**
连接到移动介质。
将“会议资料”文件保存到了移动介质。
- 17:00**
启动邮件系统。
打开新建邮件画面。
打开确认收件人画面。
- 18:00**
注销Windows。
关机。

<从日志了解到员工A的行动>

- 【9:00】PC启动**
打开PC电源,登录到Windows。
- 【9:30】确认收件箱**
早上第一件事当然是查收邮件。
启动邮件,打开收件箱。
- 【10:00】新建资料**
使用Microsoft Powerpoint编辑第二天的会议要用的资料。
同时参考了文件“调查统计结果”。
- 【12:00】Web浏览**
通过Web浏览器查看了新闻网页。
是中间休息还是收集信息?
- 【15:00】打印**
打印了上午编辑的资料。
- 【16:00】保存到外部介质**
将资料保存到了外部介质上。
这是第二天会议要用的资料,带出公司应该没问题
- 【17:00】发邮件**
启动邮件系统,打开发信画面。
大概是今天的工作报告邮件吧。
- 【18:00】关机**
关闭电源,工作结束,下班。

其他功能
~ 远程操作 ~

其他功能
~ 许可协议管理 ~

其他功能
~ 软件分发 ~

其他功能
~ 了解安全对策 ~

Q

分公司出现了系统问题！
希望尽早解决问题，可是远程操作的安全性没问题吗！？

轻易的远程操作，可能导致PC被恶意监控！

远程操作功能被使用已经有一段时间了。这虽然是非常方便的功能，可是伴随着在不知情的情况下PC被恶意操作、或者远程操作时输入的ID密码等重要信息通过网络被泄漏的危险。

A

在使用远程操作时，
验证对方身份，传输数据加密

JP1可以实现

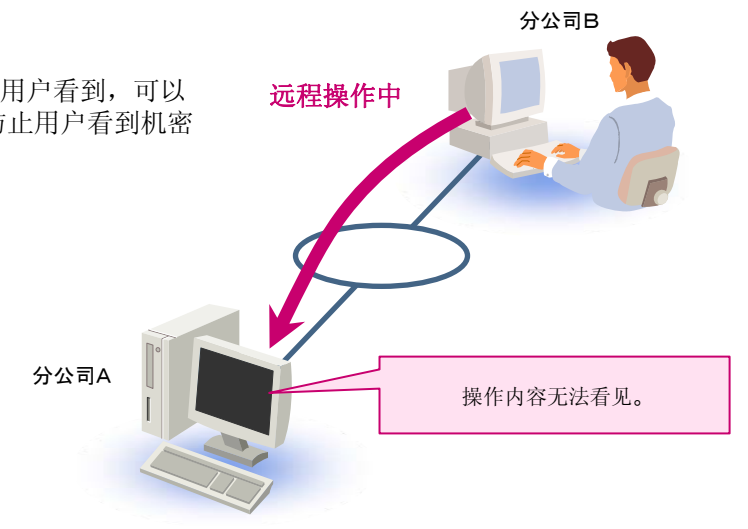
限定远程操作范围，减小被恶意利用的风险。

在远程操作连接时进行认证，只有在判断为合法用户的情况下才赋予其远程操作许可。并且，ID和密码等画面输入信息在发送时被加密保护。

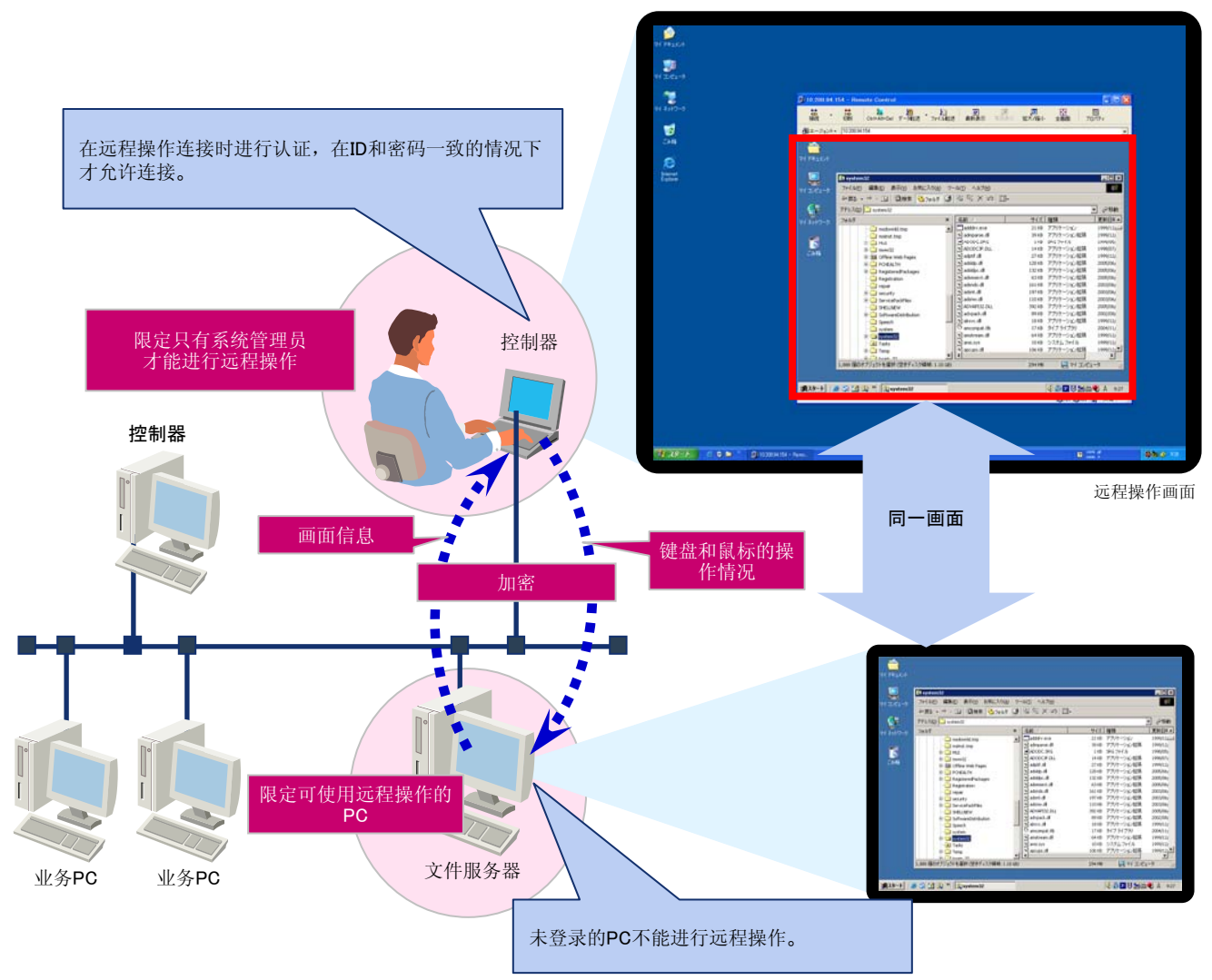
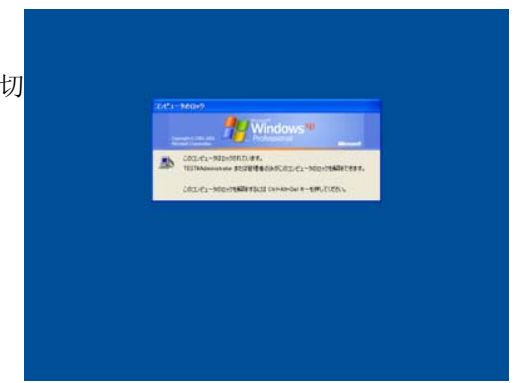
还能实现以下功能

通过以下方式强化信息安全。

- 在远程操作过程中**隐藏画面**
如果在远程操作时有些操作不便让用户看到，可以将操作对象PC的屏幕设为黑屏，防止用户看到机密操作。



- 切断远程操作时**切换到密码锁定**
当远程操作结束或者由于网络原因中断时，被操作系统可自动切换到密码保护画面，从而防止该PC被不知道密码的人随便操作。



Point! 远程操作的用户认证也可以与Windows认证功能相结合。

Point! 此外，还能将远程操作的过程录制下来。录制好的数据可以作为操作手册从主页上下载下来，也可以作为远程维护的追踪记录保存下来以备日后监视使用。

其他功能
~ 远程操作 ~

其他功能
~ 许可协议管理 ~

其他功能
~ 软件 ~

其他功能
~ 了解安全对策 ~

Q

许可协议被过度使用也没人发现！

在不考虑许可协议的情况下滥用软件，是一种违法行为！

对软件许可协议过度使用毫不知情，仍然不断的安装使用，会威胁到公司的信用。

反之，如果购买的许可协议没有被充分利用，又会导致公司的资产浪费。

可视化持有许可协议和使用许可协议的数量

JP1可以实现

轻松确认持有的许可协议是否足够

如果使用的许可协议超过了持有数，会自动发送通知邮件。还可以以部门为单位进行更细化的许可协议管理。

许可协议使用过度的软件一目了然！

ソフトウェア名	ソフトウェア種別	保有数	利用数	空数
Microsoft .NET Framework 2.0	商用	5	3	2
Microsoft .NET Framework 2.0 日本語 Language Pack	商用	3	2	1
Microsoft .NET Framework 2.0 用の Security Update	商用	1	1	0
Microsoft Excel 2000 SR-1	商用	3	3	0
Microsoft Internet Explorer 6 SP1	商用	1	1	0
Microsoft Office 2000 SR-1 Professional	商用	30	13	17
Microsoft Project 2000	商用	5	1	4
Microsoft SQL Server	商用	3	1	2
Microsoft SQL Server 2000	商用	3	2	1
Microsoft Visual C++ 2005 Redistributable	商用	10	0	10
Microsoft Visual C++ 2005 Redistributable (日本語)	商用	10	1	9
Microsoft Visual C++ 6.0 Enterprise Edition (日本語)	商用	5	3	2
Microsoft Visual J# 2.0 Redistributable Package	商用	5	0	5
Microsoft Visual SourceSafe	商用	2	1	1
Microsoft Visual SourceSafe	商用	5	1	4

即使尚未安装的软件，也能看到它的许可协议持有情况

各部门的详细信息

ライセンス区分	部署	保有数	割当数	利用数	空数	保有数累計	利用数累計	空数累計
マシン許諾	本社	10	0	0	10	30	13	17
	本社/営業部/営業1課	15	12(11)	12	3	15	12	3
	本社/営業部/営業2課	5	1	1	4	5	1	4

各部门许可协议数一览

資産番号	部署	ユーザ名	ソフトウェア名	ソフトウェア種別	インストール日
1000000134	本社/開発部/1 G	日立談計 1	Microsoft Office 2000 SR-1 Professional	商用	2008/0
1000000135	本社/開発部/1 G	日立談計 2	Microsoft Office 2000 SR-1 Professional	商用	2008/0
1000000136	本社/開発部/1 G	日立談計 3	Microsoft Office 2000 SR-1 Professional	商用	2008/0
1000000137	本社/資産管理部	日立談計 4	Microsoft Office 2000 SR-1 Professional	商用	2008/0
1000000138	本社	日立談計 5	Microsoft Office 2000 SR-1 Professional	商用	2008/0
1000000139	本社/開発部/2 G	日立談計 6	Microsoft Office 2000 SR-1 Professional	商用	2008/0
1000000140	本社/開発部/2 G	日立談計 7	Microsoft Office 2000 SR-1 Professional	商用	2008/0
1000000141	本社/開発部	日立談計 8	Microsoft Office 2000 SR-1 Professional	商用	2008/0

各用户的详细信息

各机器许可协议数一览

資産番号	ホスト名	IPアドレス	2008/01	2008/02
1000000134	asset134	10.208.93.134	0.0%	0.0%
1000000135	asset135	10.208.93.135	0.0%	0.0%
1000000136	asset136	10.208.93.136	0.0%	0.0%

各机器未使用许可协议一览

还能实现以下功能

可以看到已安装却尚未使用的软件。

了解哪些软件未被充分使用，可以将其转移到需求更高的部门，从而实现软件的有效利用。

未使用许可协议一览

ソフトウェア名	ソフトウェア種別	遊休数
Microsoft .NET Framework 2.0	商用	3
Microsoft .NET Framework 2.0 日本語 Language Pack	商用	2
Microsoft .NET Framework 2.0 用の Security Update	商用	1
Microsoft Excel 2000 SR-1	商用	1
Microsoft Internet Explorer 6 SP1	商用	3
Microsoft Office 2000 SR-1 Professional	商用	13

各部门软件使用情况以月为单位显示出来

部署	遊休数
本社	1
本社/営業部/営業1課	1
本社/営業部/営業2課	1
本社/開発部	2
本社/開発部/1 G	2
本社/開発部/2 G	2
本社/資産管理部	2

各部门的详细信息

各部门未使用许可协议一览

資産番号	ホスト名	IPアドレス	2008/01	2008/02
1000000134	asset134	10.208.93.134	0.0%	0.0%
1000000135	asset135	10.208.93.135	0.0%	0.0%
1000000136	asset136	10.208.93.136	0.0%	0.0%

各机器未使用许可协议一览

- 对于防病毒产品之类一旦服务期限结束就失去价值的软件，可以在期限结束前发出通知（任意指定）。
- 对于没有必要购买许可协议的软件（免费软件、安全补丁等），也能够了解它们的安装情况。

其他功能
~ 远程操作 ~

其他功能
~ 许可协议管理 ~

其他功能
~ 软件分发 ~

其他功能
~ 了解安全对策 ~

Q

虽然按时发出了各种软件更新指示，
但是难以把握员工是否按时更新了...

软件更新不及时也有很大风险！

出于安全考虑，如果重要程序的更新不及时，那么感染病毒或者受到外部侵犯的风险就会增大。

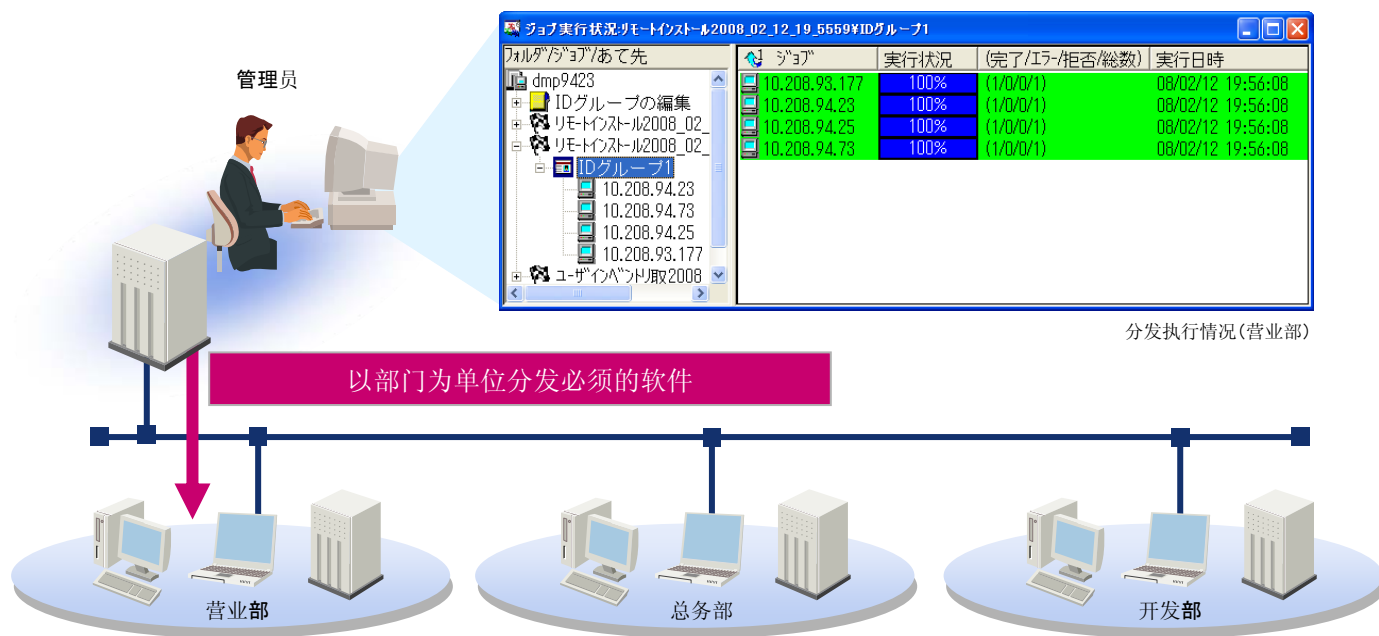
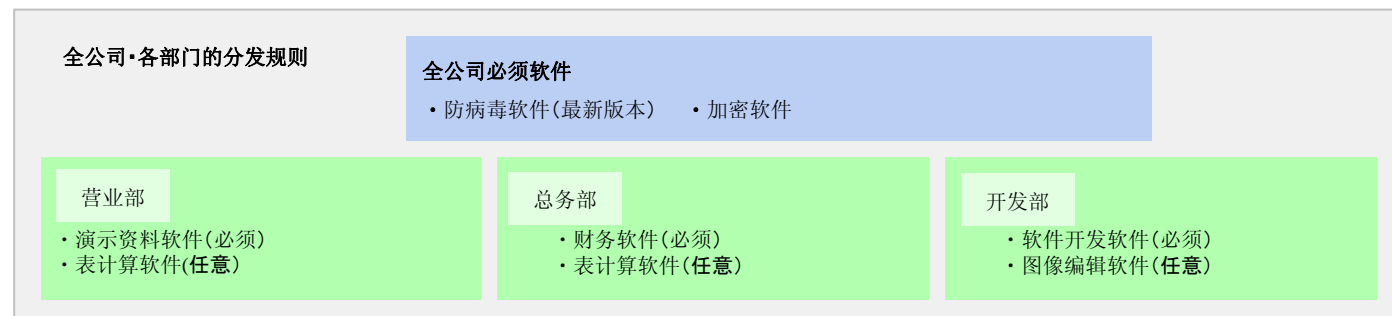
确保软件始终最新

JP1可以实现

将必要的软件分发给必需的PC

可以将必要软件强制分发到所有的客户端PC上。

可以以部门为单位分发不同的软件。



Point!

- 还可以指定日程表，全公司统一更新。
- 可自动在夜间启动PC执行分发，从而避免对日常业务造成影响。结束后可自动关机。

还能实现以下功能

从Microsoft公司获取最新的安全补丁和Service pack等的信息，然后通过简单的操作将这些更新程序分发到各个客户端。

①确认更新程序一览
选择必要的Windows补丁

②下载Windows补丁

③将Windows补丁做成分发用数据

④发出Windows补丁的分发指令

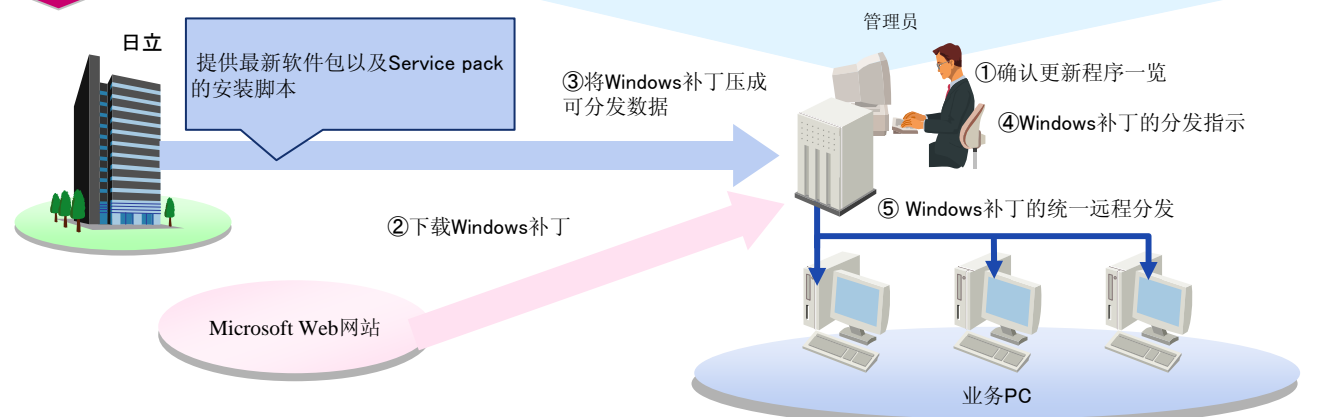
⑤Windows补丁的统一远程分发

更新程序的管理



自動作業

管理者手動執行作業



注※ 为了获取更新程序一览的最新信息，需要与日立的中间件服务V协议。

- 其他功能 ~ 远程操作 ~
- 其他功能 ~ 许可协议管理 ~
- 其他功能 ~ 软件分发 ~
- 其他功能 ~ 了解安全对策 ~

Q 虽然实施了PC安全对策，但效果如何无法确认 . . .

A **安全效果一目了然**

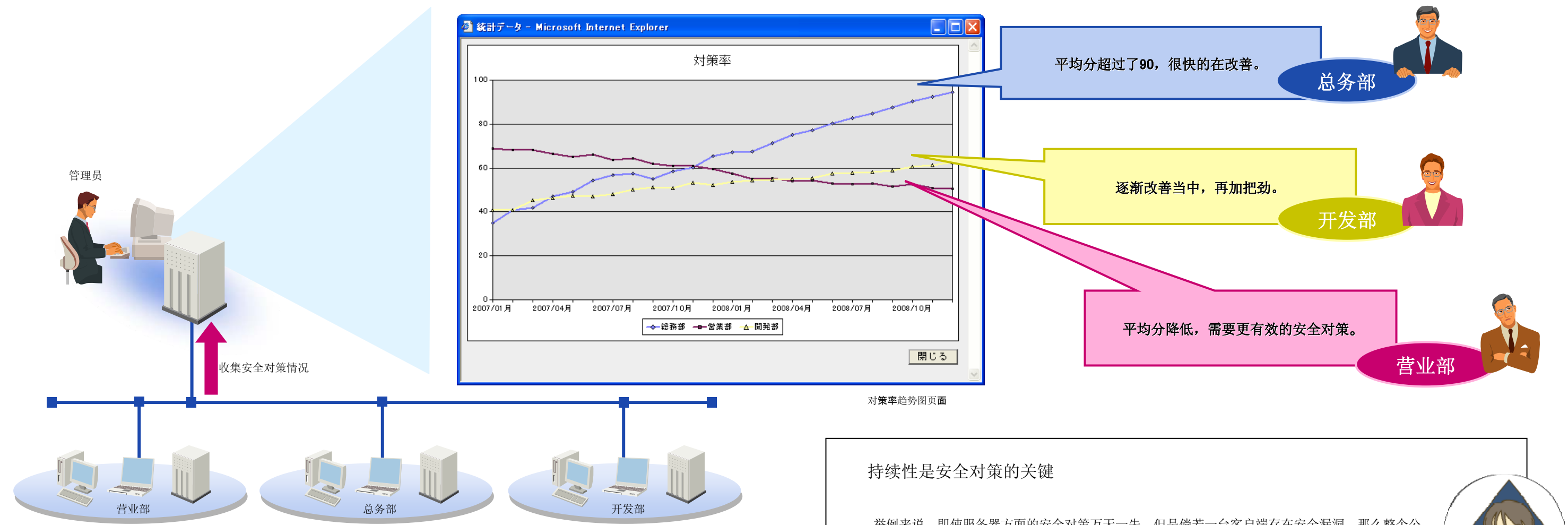
无法确认安全对策的效果的潜在风险
 系统安全所受的威胁不断递增，因此，即使实施了安全对策，如果只是临时的措施，是没有效果的。
 因此，必须随时对公司的安全对策情况进行整体把握和跟踪。

JP1可以实现

将安全对策情况的推移图表化，效果一目了然。

对公司内部的安全对策情况进行检查和分数评估。
 以部门为单位查看平均分的推移，横向把握安全对策情况。

- 还可实现以下功能
- 以图表形式显示出各个安全项目具体效果的推移情况。
 - 通过各项目的推移，判断哪个安全对策有待改善。



Point! 在所有PC中安全PC所占的比例一目了然。

持续性是安全对策的关键

举例来说，即使服务器方面的安全对策万无一失，但是倘若一台客户端存在安全漏洞，那么整个公司就会受到威胁。为了减轻这种风险，必须持续的检查和改善安全对策是一个重要的课题。

Compliance Memo