技術解説

情報セキュリティ対策 ―セキュリティホスピタル―

Information Security Solution “Security Hospital Services”

中　西　和　男*
K. Nakanishi

1. は　じ　め　に

近年，インターネットの利用の拡大，IT化の推進は目覚ましく，家電製品であるテレビ，冷蔵庫などにもインターネットを利用するものが現れ，個人でも自宅でインターネットを利用し，情報収集やコミュニケーションの手段ばかりでなくインターネット・バンキングや通信販売の利用なども行われるようになってきた。

インターネットはディジタル通信であり，基本的には規制がなく，安価に長時間の利用が可能で，また大量のデータの送受信が可能である。また，ディジタル化できればその情報はどのような内容でもよく，文字情報のほか，静止画・動画といった画像情報，MP3として利用が増えている音楽情報や通信費用が安いと言われるインターネット電話など，さまざまな情報のやりとりが可能になっている。

こうした便利さの陰で，インターネットを利用した犯罪も急増しており，すでに刑法においても**表1**に示すように情報セキュリティに関する刑罰が定められ，さらに不正アクセス禁止法（不正アクセス行為の禁止等に関する法律）が1999年に成立し，2000年2月から施行されている。

表1 刑法に定める情報セキュリティ関係の刑罰規定

第161条の2	電磁的記録不正作出及び供用
第234条の2	電子計算機損壊等業務妨害
第246条の2	電子計算機使用詐欺
第258条	公用文書等毀棄
第259条	私用文書等毀棄

本稿では，この不正アクセスの動向を概観した後，その不正アクセス対策をサポートし，セキュリティ評価や設計，セキュリティ機能の実装などを提供するため当社で開発したセキュリティホスピタル（商標登録出願中）・サービスを紹介する。

セキュリティホスピタル・サービスとは，お客さまにそのセキュリティレベルを適切に維持していただくためのプロセスの維持，改善のための支援を行うものであり，セキュリティ評価から不正アクセス緊急対応に至るすべてのプロセスをカバーしている。

2. 不正アクセス

2・1 不正アクセス

不正アクセスには，不正アクセス禁止法の第3条（**表2**）に規定されている狭義の不正アクセスと，広義の不正アクセスがある。広義の不正アクセスには，コンピュータを直接操作し情報を盗み出したり，消去したり，正規の利用者の利用を妨害したり，あるいは詐欺，人権侵害などにコンピュータを利用するといった行為がある。この場合，現在の法制度では刑法に頼ることになるが，刑法では操作権限を持たない者が「単に操作した」だけでは罰することはできない。

一方，狭義の不正アクセスは，不正アクセス禁止法の第3条で「電気通信回線を通じて」行われる不正アクセスに限定している。この場合には，実害がなくてもアクセスを行っただけで処罰の対象になり得る。

ここでは，この狭義の不正アクセスについて，その発生状況や脅威について示す。

2・2 不正アクセス事件の発生状況

国家公安委員会，総務大臣，経済産業大臣による2001年2月9日の公表によれば，不正アクセス禁止法での検挙件数は，2000年2月13日に同法が施行されてから2000年12月31日までで31事件，検挙された者は37名にも及んでいる。検挙されないまでも警察庁に報告された不正アクセス行為は106件にもなる（**表3**）。

実際に検挙された31の事件についてその犯行の手口を見ると，他人のID，パスワードを不正に利用したケ

* 情報通信開発事業部 品質保証課

ースが30件で，残り1件がコンピュータなどのセキュリティ・ホール攻撃，つまりコンピュータの弱点を突いた攻撃である。ただし，セキュリティ・ホール攻撃を行ってID，パスワードを取得し侵入した場合も30件の中に数えられている。

これらの不正アクセス事件でID，パスワードがどのようにして不正に入手されたかについては，**表4**のとおりとなっている。

なお，JPCERT/CC（コンピュータ緊急対応センター）への不正アクセスに関する報告件数は，**図1**に示すとおりである。この数字は，未遂，重複した報告もあるため不正アクセス事件の件数を直接に示すものではないが，不正アクセスが急増していることをうかがわせる。

これらの不正アクセスは，インターネットを利用して行われることから，国内だけに限らず，世界各国から行われているものと思われる。日本では，2000年1月から2月にかけての官公庁のホームページ改ざん，2001年2月の民間企業各社のホームページ改ざんがあり，ともに多くの組織のホームページが短期間のうちに書き換えられるという被害を受けた。これらは外国からの不正アクセスだと言われている。

表2 不正アクセス禁止法抜粋

（不正アクセス行為の禁止）
第3条　何人も，不正アクセス行為をしてはならない。
2　前項に規定する不正アクセス行為とは，次の各号の一に該当する行為をいう。
一　アクセス制御機能を有する特定電子計算機に電気通信回線を通じて当該アクセス制御機能に係る他人の識別符号を入力して当該特定電子計算機を動作させ，当該アクセス制御機能により制限されている特定利用をし得る状態にさせる行為（当該アクセス制御機能を付加したアクセス管理者がするもの及び当該アクセス管理者又は当該識別符号に係る利用権者の承諾を得てするものを除く。）
二　アクセス制御機能を有する特定電子計算機に電気通信回線を通じて当該アクセス制御機能による特定利用の制限を免れることができる情報（識別符号であるものを除く。）又は指令を入力して当該特定電子計算機を作動させ，その制限されている特定利用をし得る状態 にさせる行為（当該アクセス制御機能を付加したアクセス管理者がするもの及び当該アクセス管理者の承諾を得てするものを除く。次号において同じ。）
三　電気通信回線を介して接続された他の特定電子計算機が有するアクセス制御機能によりその特定利用を制限されている特定電子計算機に電気通信回線を通じてその制限を免れることができる情報又は指令を入力して当該特定電子計算機を作動させ，その制限されている特定利用をし得る状態にさせる行為

表3 不正アクセスの警察庁への報告件数
（2001年2月9日の国家公安委員会，総務大臣，経済産業大臣による公表から）

被　害　者	件　数
プロバイダ	59件
大　学	8件
情報通信企業	6件
その他	33件
計	106件

表4 ID，パスワードの不正入手の方法
（2001年2月9日の国家公安委員会，総務大臣，経済産業大臣による公表から）

不正入手の方法	件数
ID，パスワードの管理の甘さにより入手	12件
セキュリティ・ホール攻撃により入手	8件
他人からID，パスワードを入手	6件

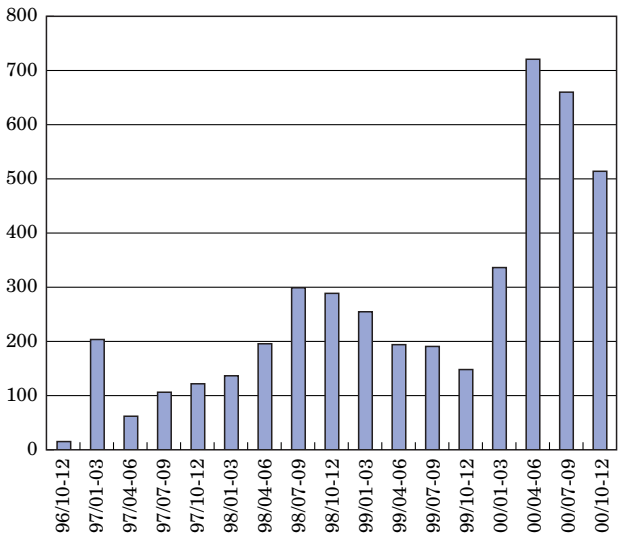


図1 JPCERT/CCに届けられた不正アクセスの報告件数

2・3 不正アクセスの脅威

このような不正アクセスの多くは，**図2**に示す手順を追って行われるものと見られる。これまでの国内での不正アクセス事件では，ホームページの書き換えが大きく報じられており，機密情報が盗まれたといった確たる報道は行われていない。ただ，元のデータがコピーされるだけでは証拠がつかみにくいため，データを盗まれたかどうかの判断は極めて困難な場合が多い。海外での不正アクセス事件では，クレジットカード番号を大量に盗まれた等の事件も報告されている。

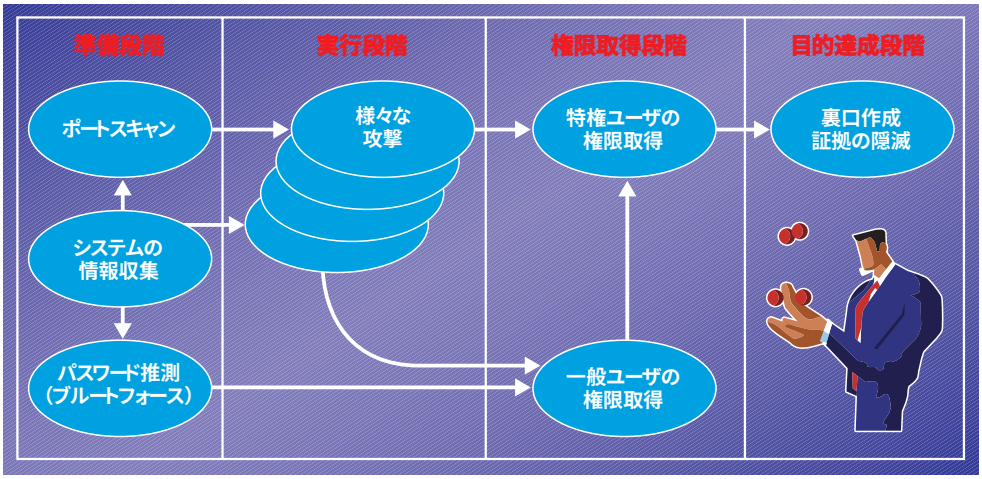


図2　一般的な不正アクセスの手順

通常，ホームページの改ざんは，ホームページを開設しているコンピュータに侵入し，ホームページに相当するファイルを書き換えたり，別のファイルにすり替えたりすることで行われる。つまり，ホームページの改ざんがあったということは，そのコンピュータを自由に操作できる権限が乗っ取られたと考えても良い。

したがって，一つのコンピュータでもそのような乗っ取りに合うと，そのコンピュータに接続されている他のコンピュータも次々と乗っ取られる可能性が高くなり，機密データが外部に漏れたり，重要なデータが破壊されたり，あるいは工場やプラントを制御しているコンピュータが誤動作させられるなどの大きな被害を被ることにつながる。

ある試算によると，企業が不正アクセスを受けた場合の被害額はその企業の年間売上の6％から7％にもなるとされている。もしこれが日常の業務に不可欠な重要なデータの破壊であったり，顧客データなどが流出し損害賠償請求を受けた場合などは，何十億円といった莫大な被害額になる可能性もある。

これらの脅威を考えると，まだ不正アクセス被害を受けていないからといって安心することはできず，被害を受ける前に十分な対策を講じる必要がある。

3．不正アクセス対策

このような不正アクセスに対処するには，ファイアウォールに代表されるような防御用機器やソフトウェアを導入することはもちろんであるが，使用しているプログラムについて常に情報を収集し，セキュリティ・ホールが発見され対処方法が示されたものについては，速やかにその対応を行わなければならない。

このような不正アクセス対策は，ある程度の対策を実施すると，それ以降は費用がかさむばかりで，かける費用ほどの効果が得られない可能性もある。したがって，その組織や保護するべきデータ，情報，あるいはネットワークの運用方法に応じて，妥当なレベルでの対策を実施することになる。

そのためには，まず組織のセキュリティ・ポリシー（方針）を定めること，すなわち，組織としてどの情報をどの程度守るのかという方針をセキュリティ・ポリシーとして明らかにしなければならない。さらにそのポリシーに基づいて具体的に実施する対策や管理方法を基準や内部規程として定め，さらに，それを防御用機器の設定方法や監視の方法として具体的手続きを定めることが求められる（**図3**）。このとき，防御策と管理策の両面で対処しなければ現実的な対応策は得られない（**図4**）。

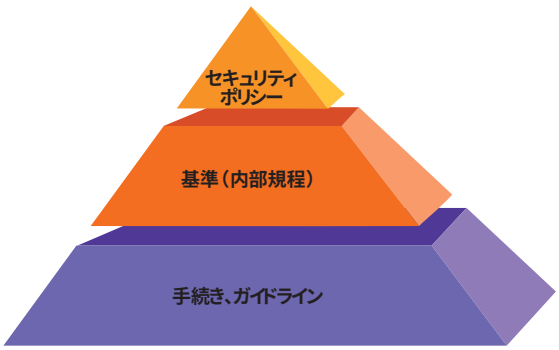


図3　セキュリティ・ポリシーと基準，手続き

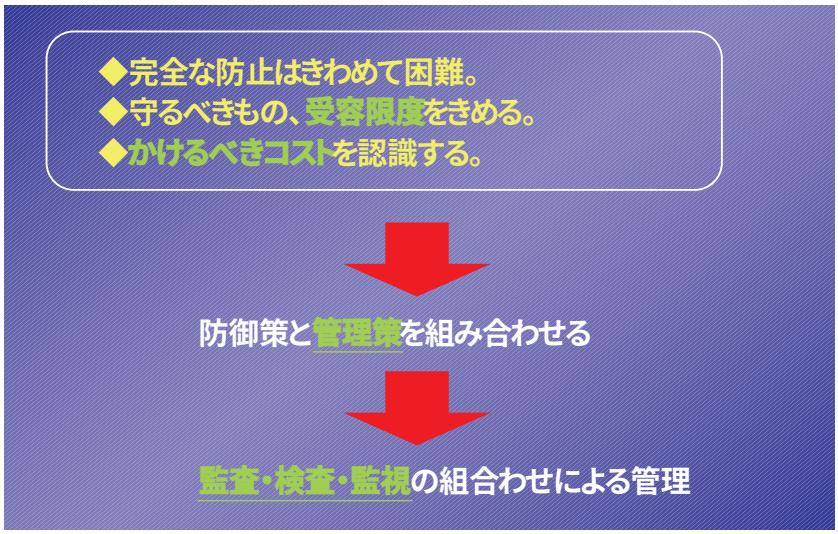


図4　セキュリティ対策の考え方

このとき，セキュリティ対策としては，

①抑止（不正アクセスが生じない仕組み作り）
②予防（不正アクセスを防止する方法）
③検出（不正アクセスを早期に検出し，対応できるようにする方法）
④回復（不正アクセスによる被害を原状に復帰する方法）

の四つの観点で検討すると良い。

さらに，基準（内部規程）には，セキュリティ対策の実施状況や防御用，監視用機器の設定内容について定期的な監査を行うような規定を盛り込むべきである。もし，定期的な監査の結果，適切なセキュリティ対策が行われていないことが見つかればそれを是正する必要がある。その是正処置には，基準（内部規程）や手続きの修正，改善もその範囲に入る。

このような考え方から，**図5**に示すライフサイクル・セキュリティという概念が必要になってきた。情報セキュリティに関して，一旦，防御対策を行った場合，それで安心してしまうケースが時折見られる。不正アクセスの手口は，常に巧妙になりつつあり，また組織の業態，活動内容なども変化し続けていることを考えると，ぜひとも情報セキュリティに関して，ライフサイクル・セキュリティを念頭に置かなければならない。

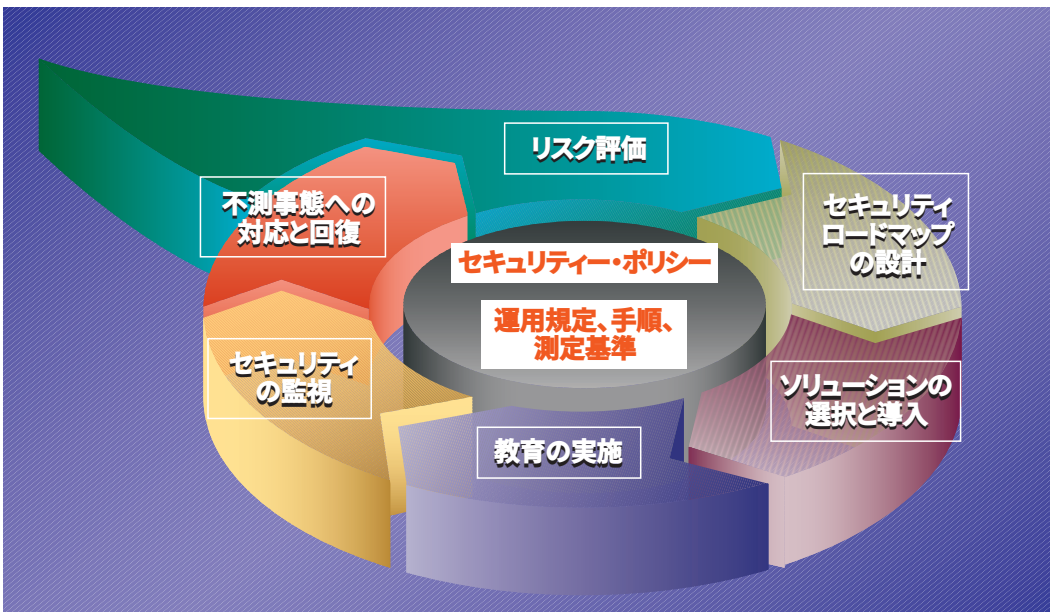


図5　ライフサイクル・セキュリティ

4．セキュリティホスピタル

当社では，従来から情報セキュリティ対策として，**表5**に示す製品をお客さまに提供し，セキュリティ対策を「モノ」の面から支援してきた。

表5　当社のセキュリティ対策製品

プロテクト	ファイアウォール	CyberGuard Firewall（ISO15408：EAL4）	CYBERGUARD
	暗号通信	LANBASE SX20（IDEA暗号）	ELNIS
		PowerVPN（リモートアクセス対応）	
	認証	Defender（使い捨てパスワードシステム）	
アセス	●監査 ●検査	ESM：セキュリティポリシーとの一致を監査 NetRecon：セキュリティの弱点を検査	symantec.
モニタ	●監視（対抗）	ITA：ホストベースで不正アクセスを検知・排除 NetProwler：NW上で不正アクセスを検知・排除	

すなわち，ファイアウォールや暗号通信用機器，認証の仕組みによって防御装置・システムを構築できるようにし，お客さまの情報システムに対する監査ツールや検査ツールを提供して不正アクセスの危険性を評価できるようにし，さらに監視ツールによって不正アクセスを検知できるようにしてきた。

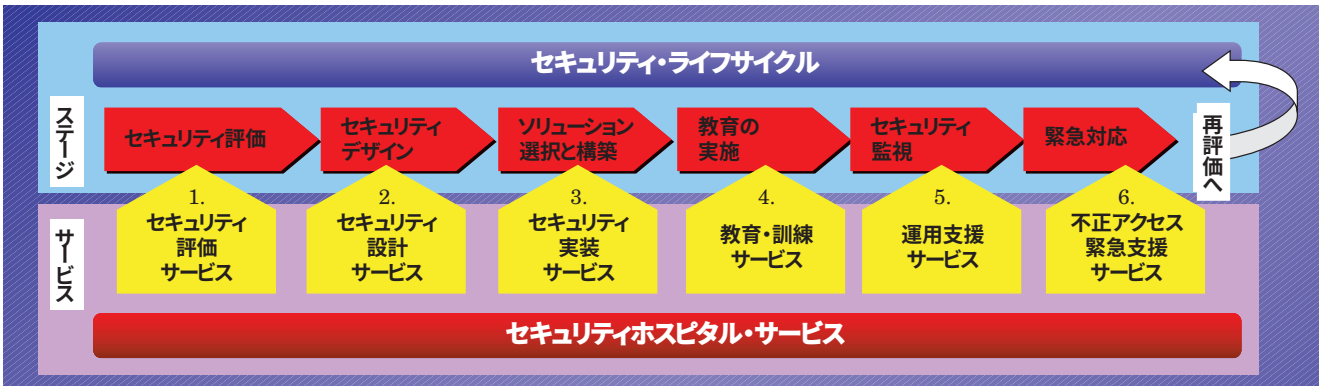
当社では，前述のようなライフサイクル・セキュリティの重要性を考慮し，これらの情報セキュリティ対策製品に加えて，情報セキュリティの確保に努力しているお客さまに**図6**に示すセキュリティホスピタル・サービスを提供している。このセキュリティホスピタル・サービスは，情報セキュリティ対策製品と車の両輪を構成する重要なサービスである。

(1) セキュリティ評価サービス

お客さまのシステムについてのセキュリティ評価を行うサービスである。ISO 15408（Common Criteria）やBS 7799，あるいは国内外のセキュリティ関係の基準などに盛り込まれている重要項目を取り入れたチェックシートと，表5に示したような評価のための監査ツール，検査ツールなどを用いてお客さまのシステムのリスク評価および対策の提案を行う。

(2) セキュリティ設計サービス

セキュリティ評価サービスによってお客さまのシステムに対するセキュリティ評価を行った結果や監査結果をもとに，そのシステムのセキュリティを具体的にどのようにして改善するのかを提案するとともに，お客さまのセキュリティ・ポリシーに基づいてOSプラットホームに関する手続きレベルの監視や監査項目のカスタマイズ，不正アクセスを検知するための不正アクセス・パターンのカスタマイズ等のサービスを提供する。このセキュリティ設計サービスでは，お客さまのセキュリティ・ポリシーの作成についての支援も行う。



1. セキュリティ評価	ISO15408（CC），BS7799の重要評価項目を取り入れたチェックシートおよびセキュリティ管理ツール等によるリスク評価と対策
2. セキュリティ設計	セキュアなネットワーク設計を含めた最適なセキュリティデザイン提案、カスタマイズ
3. セキュリティ実装・カスタマイズ	製品インストールや動作確認、最適な動作設定
4. 教育・訓練	オペレーショントレーニング
5. 運用支援	●ネットワークのセキュリティ設定の適切性診断、監視項目の最適化 ●ファイアウォールのログ解析、侵入検知システムの警報の種類・危険度等についてのコンサルテーション
6. 不正アクセス緊急対応	不測の事態発生時の、リカバリー支援サービス

図6　セキュリティホスピタル

(3) セキュリティ実装サービス

情報セキュリティ対策機器やソフトウェアが高度化，複雑化している中，それらの機器やソフトウェアのインストール，動作確認，およびお客さまのポリシーやシステムに合わせた最適なセキュリティに関する設定を行うサービスである。

(4) 教育・訓練サービス

主として，セキュリティ対策機器やソフトウェアについてお客さまのサイトでお客さまのシステムに合わせた内容でのオペレーション・トレーニングを行う。

(5) 運用支援サービス

お客さまのシステムを運営する上で，システムの変更，世の中のセキュリティ事情の変化などに合わせてより適切なセキュリティ対策とするために，侵入検知・監視システムやファイアウォールなどの設定情報の見直し・修正，出力されるログの解析，および不正アクセスについての警報の種類や危険度に関するコンサルテーション等の支援を行う。

(6) 不正アクセス緊急支援サービス

万一，不正アクセスを受けたときにお客さまが行う緊急対応についての支援を行う。

5. お わ り に

セキュリティ対策は，機器やソフトウェアの導入のみでは完璧にはならない。それらの機器やソフトウェアの適切な利用とお客さまの組織や人の管理などの面が相まって初めて効果的なものとなる。また，不正アクセスを試みる者も日々工夫し続けている。このため，セキュリティ評価を少なくとも定期的・継続的に実施し，その結果を実際のセキュリティ対策機器の設定や組織の運用・管理面に反映させる必要がある。すなわち，セキュリティ対策はプロダクトで終わるのではなく，日頃の対策実施のプロセスそのものである。

当社が提供するセキュリティホスピタル・サービスは，お客さまにそのセキュリティ・レベルを適切に維持していただくためのプロセスの維持，改善のための支援を行うものである。今後もセキュリティホスピタルで提供するサービス・メニューをより充実させ，より確実なセキュリティ対策を提供していく。

なお，情報セキュリティに関しては，次のような基準，指針などがある。お客さまの情報システムのセキュリティ対策を検討する上で参考にしていただきたい。

－ISO 15408：Common Criteria　（JIS X 5070：情報技術セキュリティの評価基準）
－BS7799：Information security management
－ISO/IEC TR13335：Information technology －Guidelines for the management of IT Security
－JIS Q 15001 個人情報保護に関するコンプライアンス・プログラムの要求事項
－情報システム安全対策基準（平成7年通商産業省告示第518号）
－情報システム安全対策指針（平成9年国家公安委員会告示第9号）
－コンピュータ不正アクセス対策基準（平成8年通商産業省告示第362号）
－コンピュータウイルス対策基準（平成9年通商産業省告示第535号）
－民間部門における電子計算機処理に係る個人情報の保護に関するガイドライン
（平成9年通商産業省告示第98号）
－電気通信事業者における個人情報保護に関するガイドライン（平成10年郵政省第570号）
－不正アクセス行為の禁止等に関する法律（平成11年法律第128号）
－不正アクセス行為の再発を防止するための都道府県公安委員会による援助に関する規則
（平成11年国家公安委員会規則第12号）

◆ **執筆者紹介**

中 西 和 男　情報通信開発事業部 品質保証課 課長