エレクトロニックコマース・セキュリティ特集

UDC 342.738：681.324(100)

インターネット時代の情報セキュリティ

IT Security in Internet Age

松井一成 Kazushige Matsui　八田孝夫 Takao Hatta　芦田元之 Asanobu Ashida

要　旨

インターネットを利用したビジネスのために不可欠な情報セキュリティについて，脅威と対策の概要を述べる。

1．まえがき

インターネットに代表されるオープンネットワーク環境を利用したイントラネット／エクストラネットシステムが急速に発展し，企業間や消費者向けのインターネットコマースが一般化し，ビジネスに急激な変化をもたらしつつある。一方，2000年１月頃から多発した官公庁のウエブシステムに対する不正アクセス等の各種コンピュータ犯罪により，情報セキュリティの必要性が改めて認識された。インターネット･ビジネスを成功させるためには，情報セキュリティがキーとなる。

21世紀には，インターネットは，企業だけでなく家庭などどこからでも，いつでも簡単に利用でき，現在の電話網のような世界共通のユニバーサル･ネットワークになると考えられる。このインターネットを中心としたネットワーク社会において，不可欠なものが情報セキュリティ対策である。情報セキュリティ対策は，Y2K問題に区切りがついた今，これから取り組まなければならない最重要課題である。

2．情報セキュリティ対策の必要性

従来，情報セキュリティの範囲が不明確であり，システム導入時にビジネスへの貢献度が測定できないこと，利便性が悪く，運用が複雑であること，費用対効果が見えないことから，情報セキュリティの必要性は感じられながらも軽視されがちであった。

ファイアウォールを設置すれば情報セキュリティ対策は十分であると考えている人が多いと思われるが，これは間違いである。ファイアウォールはインターネットからのアクセスを制御をするが，ウエブサーバのセキュリティホールを利用した不正アクセスに対しては無力である。また，コンピュータ犯罪の80%以上は内部犯行であるといわれているが，これに対しても無力である。

情報システムは，常にコンピュータ犯罪の脅威にさらされている。コンピュータ犯罪に対応するためには，脅威分析に基づいて，運用，コスト，利便性のバランスを考えたセキュリティソリューションが必要である。

3．情報セキュリティの脅威と対策

情報セキュリティ上の脅威は，第三者による悪意のある意図的な脅威であり，天災，誤動作や故障等の偶発的な脅威は含まない。情報セキュリティ上の脅威は，以下の３つに分類できる。

１）データの機密性（Data Confidentiality）に対する脅威；ネットワーク上のデータやサーバ上のデータを許可されていない人に見られること。


松井一成
システムソリューションカンパニー ビジネスソリューション事業部長


八田孝夫
システムソリューションカンパニー ビジネスソリューション事業部 副事業部長


芦田元之
システムソリューションカンパニー ビジネスソリューション事業部 情報セキュリティ担当部長

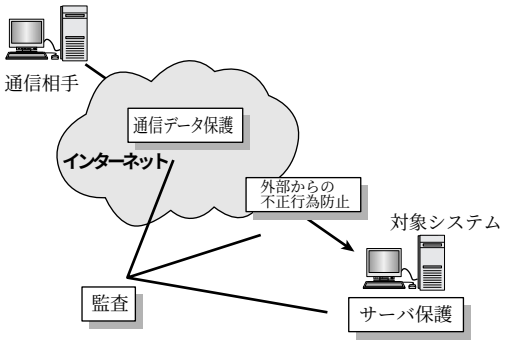

図１　情報セキュリティ対策
Fig. 1　Countermeasures for IT security

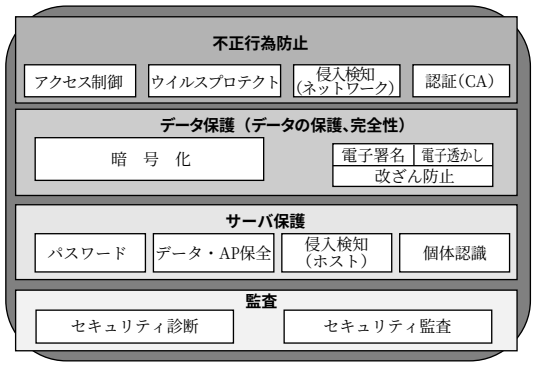

図２　情報セキュリティ対策技術のフレームワーク
Fig. 2　Framework of IT security technology

2）データの完全性（Data Integrity）に対する脅威；ネットワーク上のデータやサーバ上のデータが不当に改ざんされたり，破壊されること。
3）情報の可用性（Availability）に対する脅威；システムの機能，サービス，データが，悪意のある人によって利用できなくされること。

これらの脅威に対する情報セキュリティ対策は，インターネット上を流れる通信データ保護，外部からの不正行為防止，サーバ保護およびシステム監査がある（図１参照）。

保護対象システムに対して，セキュリティ管理･評価とセキュリティ対策技術の両面から対策を行なう必要がある。

4．セキュリティ管理･評価

セキュリティ管理･評価は，間接的なセキュリティ対策であり，以下の方策からなる。

1）セキュリティポリシー；企業の情報セキュリティに対するガイドラインであり，情報資産に対する脅威分析に従って，対応策の基準を決める。このセキュリティポリシーに従って，システム開発･運用およびセキュリティ教育を行なう。
2）セキュリティ評価基準（CC：Common Criteria）；セキュリティ要求仕様書に従って製品／システムが設計され，セキュリティ機能が漏れなく実装されているかを評価するための基準である。

セキュリティ評価基準は，1999年６月にISO化され，2000年７月にJIS化が予定されている。沖電気は，セキュリティ評価基準を取り込んだ開発プロセスを社内技術標準としている。

5．情報セキュリティ対策技術

情報セキュリティ対策技術は，直接的なセキュリティ対策である。図２に，情報セキュリティ対策技術のフレームワークを示す。

不正行為防止技術は，外部からシステム内への不正アクセスや侵入を防止する技術である。データ保護は，データの機密性や完全性を保証するための技術である。サーバ保護は，サーバの機能，サービスおよびデータを保護し，システムの可用性を高める技術である。沖電気は，これらの技術の中で特に，未知のアタックに対応できる侵入検知，改ざん防止と原本性を保証するための電子透かし，目の虹彩を利用した個体認識に注力している。

6．あ　と　が　き

日本における情報セキュリティ対策は米国に比べて数年遅れていると言われている。特にセキュリティポリシーは，米国の企業では当たり前であるが，日本では一握りの企業でしか定められていないのが現状である。

情報セキュリティを強化すればするほど利便性が悪くなる。また，いくらコストをかけても，100%の情報セキュリティは達成できない。インターネットを利用したビジネスにおける脅威分析を行ない，情報セキュリティの強度，コストおよび利便性のバランスを考慮した，トータルな情報セキュリティソリューションを開発しなければならない。

沖電気は，米国の最新技術を導入したセキュリティ・トータルソリューションを提案している。