セキュアOSを導入せよ～セキュリティ対策の限界を越える

日本高信頼システム研究所
主任研究員　田口　裕也

『セキュアOSの必要性』

「セキュアOSの導入を。」このような言葉が内閣官房情報セキュリティセンターの報告書「電子政府におけるセキュリティに配慮したOSを活用した情報システム等に関する調査研究」に提示され、「セキュアOS」を使用するべきと明示されました。この発表の背景には、数々の著名な企業のWebサイトが不正アクセス、不正侵入を受け、多くの情報が漏洩したり改ざんされる被害報告を多く聞く深刻な事態があったからです。これらの被害を受けたシステムの状況を調べてみると、必ずしもセキュリティ対策を怠っていたというわけではありません。通常は、構築するシステムにセキュリティ対策を施すことは「当然のこと」として認識されています。アンチウィルスやファイヤーウォール、IDSなど、いろいろな製品を組み合わせて、考えられる脅威からシステムを保護することはあたりまえの時代です。しかし、攻撃を受けてしまうといとも簡単にシステムが侵略され、企業にとってとても大切なお客様の個人情報や、経営にかかわる機密情報などがあっさりと外部に漏れてしまうのが現状です。このように、最近の著しいインターネットの普及に伴い、多くの事故やさまざまな脅威からシステムを保護するためのセキュリティ対策に注目が集まっています。その中でも、OSのセキュリティについては、より信頼性のあるシステムを構築するために特に注力しなければならない項目として政府から取り上げられているのです。今回は現在のセキュリティ対策になぜOSセキュリティが追加で必要なのか、また、政府が導入を促進しているセキュアOSとはどのようなものなのかを開発された歴史をたどり、OSそのものを強靭にする必要性を解説します。

1. 現在のセキュリティ対策の抜け道

近年のセキュリティ対策では、たくさんの導入費用と時間を使い、アンチウィルスやファイヤーウォール、IDSなどで、何重ものセキュリティ対策をすることは当然であると思います。これらの対策方法で大切な情報を格納しているシステムを間接的に守ろうとしていました。ネットワーク周辺からシステムを保護することによって、不正なアクセスを防止するアプローチです。しかし、これらのセキュリティ製品のほとんどが一般に公開されていない未発見のウィルスや、脆弱性への攻撃、また、脆弱性を直すパッチがリリースされるまでの対策ができない期間に対しては無意味に近いのではないかと言われています。なぜなら、ウィルスや不正な攻撃を事前に防ぐためには、世界中で発見されたたくさんの攻撃手法をパターンとして登録しているパターンマッチングという方式で動作している製品がほとんどだからです。もし、あらかじめ定義された攻撃手法のパターンと同じ攻撃が発生すれば、もちろんシステムを守ってくれますが、これらの防御機能を常に維持するためには、パターンを登録しているパターンファイルを最新の状態に更新しつづけなければならないのです。つまり、使用しているパターンファイルに定義されていない攻撃をシステムが受けた場合、当然ながら防ぐことができません。パターンに登録されていないので認識することができないため、問題なく通過してしまうのです。

そのため、現在のセキュリティ対策では抜け道が存在し、せっかく導入したセキュリティ対策も一瞬のうちにして無意味になってしまう可能性があるのです。多額の費用と時間をかけても思うように効果が現れないのはこの仕組みのためです。

また、実装しているたいていのアプリケーションには脆弱性（バグ）が発見され、修正パッチが多く提供されています。パッチを適用すれば不具合が修正されるのですが、そのためには稼働マシンへ適用す

る前にテスト機でパッチを適用し、システムに問題がないかを検証する段階を経ます。では、脆弱性が発見されてからパッチが提供されるまでの期間はどのようにしてシステムを保護すれば良いのでしょうか。現状ではパッチが提供されていない期間はシステムを保護する手立てはほぼ皆無に近いのです。つまり、パッチの提供を待っている間は不正なアクセスや攻撃を受ける危険性が高まり、とても不安定な状態で運用しなければなりません。さらに、世間一般には公開されていない脆弱性を発見されて、攻撃を受けたとします。これは、パッチそのものが最初から存在しないため防ぎようがありません。パッチマネージメントにおける未提供期間の問題は、現状の方式では対策が不可能であるため攻撃からシステムを守ることはできないのです。

2. OS の構造上の抜け道

現状の対策では、システムの内部に不正なアクセスを許してしまうと、保存されている大切な情報は全て漏洩する可能性がとても高いことがあります。これは OS の仕組みが根本的に全ての情報へアクセスできてしまう構造で作られている現実があるためで、機密度がとても高い情報を守るためには適切なアクセス制御の設定ができません。つまり、システム全体へのアクセス権を許可されている root ユーザや Administrator（システム管理者）の存在があるからです。もし攻撃を受けた場合、必ず犯人はシステムの管理者権限を奪取しようと試みます。奪取されてしまうと、保存している全ての情報にアクセスされてしまうため、システム全体に被害が発生します。つまり、これまでの OS を使用していたのでは、まったく無防備な状態で情報は保存されている状態に近いのです。この仕組みは全ての OS にあてはまります。OS そのものが貧弱すぎると、いくらネットワーク周りでセキュリティ対策をしても無意味なのです。例えば、家を建築するときにはコンクリートで基礎をしっかり作ります。基礎を作らず砂漠の砂の上にいくら立派な家を建ててもすぐに傾いて倒壊してしまいます。同じようにシステムを構築するためにも OS（システムの土台）が頑丈でなければ信頼性の高いシステムは構築できません。OS の問題を解決するためには、普通の OS を使用していたのでは構造上の問題からすでに限界であり、解決することができません。そのため、これまでにはまったくない概念を取り入れて対策をする必要があります。

3. 注目されるセキュア OS

民間企業にも情報保護のためにいままで以上に高度なセキュリティ対策が求められています。お客様の情報を漏洩した場合の社会に与える影響や、悪用され被害が発生した場合の賠償など、「システムを守る」ことは、企業経営に関わる影響がとても大きいのです。このことから「システムを守れない」ことは一定期間の業務停止など、経営の危機に発展することもありえるのです。

そこで、現状の対策ではすでにいくつもの限界が見えてきたことから、OS そのものを強靭にして、システムを保護する「セキュア OS」が話題になり始めています。

4. セキュア OS とトラステッド OS

日本では最近セキュア OS が注目を集めるようになりましたが、実は米国では 20 年以上前からすでに製品化され、政府機関や民間企業に提供されていました。1985 年に米国防総省指令として発令された TCSEC（Trusted Computer System Evaluation Criteria：セキュリティ機能評価基準書）というセキュリティ製品の機能を評価する規格が策定されているのです。

これは、米国の国防に関わる機関へシステムを導入するためには、TCSEC に規格されているセキュリ

ティ強度を満たしていなければならないという機能を評価する規格です。

この規格は A を最上位とした Division と呼ばれる４つの階層（A、B、C、D）に分かれており、さらに各 Division ごとに class と呼ばれる７つの階層（B1、B2、B3 数値が高いほうが上位）で分類されています。（図１）

Division	Class	代表的な評価基準
D	なし	TCSEC の評価に値しない製品
C	C1	任意アクセス制御を実装
	C2	C1 に監査機能等の実装を追加
B	B1	C2 に強制アクセス制御の実装
	B2	B1 に構成管理機能の実装を追加
	B3	B2 にリカバリー機能の実装を追加
A	A1	B3 に配布時の保証機能の実装を追加

図1 TCSEC におけるセキュリティ機能の評価分類

この TCSEC で B Division で定義されている規格をクリアした OS のことをトラステッド OS（Trusted OS）と呼んでいます。

今日のセキュリティ評価基準は「ISO/IEC15408」が国際的な規格の基準となっていますが、TCSEC で定義されている多くの規格をベースとし、プロテクションプロファイルとして継承されてます。日本でもトラステッド OS を入手することはもちろん可能でした。しかし、もともと国防 (軍用システム) 向けに開発された経緯もあって、あまりにも高すぎるセキュリティ機能は、当時の民間企業へはあまり普及しなかった現実もあります。しかし、最近の情報保護を民間企業に求める動きから高度なセキュリティ対策が必須となってきました。そのため、トラステッド OS は再び注目を集めています。さらに時代の流れに合わせて登場したのがセキュア OS です。セキュア OS はトラステッド OS の高いセキュリティ機能を保ちつつ、民間企業が要求する便利な機能を次々と実装し、導入、運用しやすいようにたくさんアレンジされています。そのため、セキュア OS は厳密に TCSEC の規格を満たしているとはいえませんが、普通の OS では解決できなかったセキュリティの問題点を解決する手段として、その必要性が認知されてきています。

5. 強制アクセス制御と任意アクセス制御

実際にセキュア OS やトラステッド OS を、普通の OS と比較したとき、どの機能が大きく異なるのかと言うと、システム管理者であっても回避することのできないアクセス制御機能を実装している点です。これを、強制アクセス制御（MAC : Mandatory Access Control）と呼びます。B Division では、強制アクセス制御機能を実装することを必要な条件として定義していますが、どのような機能なのでしょうか。

これには、現在の OS が実装しているアクセス制御の仕組みを理解するととても分かりやすくなります。普通の OS ではファイルの所有者がどのユーザクラスに対して必要なアクセス権を許可するのかという設定をしてアクセス制御を行います。これを任意アクセス制御（DAC : Discretionary Access Control）と呼びます。

しかし、任意アクセス制御の大きな欠点は、一般ユーザにのみ有効なアクセス制御機能であり、システム管理者にはまったく無効であることです。つまり、設定されているアクセス権を無条件に回避することができます。これは、システム全体へのアクセス権をシステム管理者は保持している意味を表します。例を上げると、もしファイルの所有者が読み取り専用のファイルと設定しても、システム管理者はファイルの所有者の許可なく無断で書き込むことができてしまうのです（図 2)。

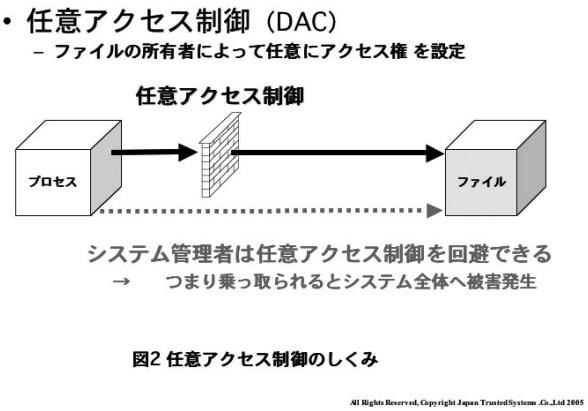

図2 任意アクセス制御のしくみ

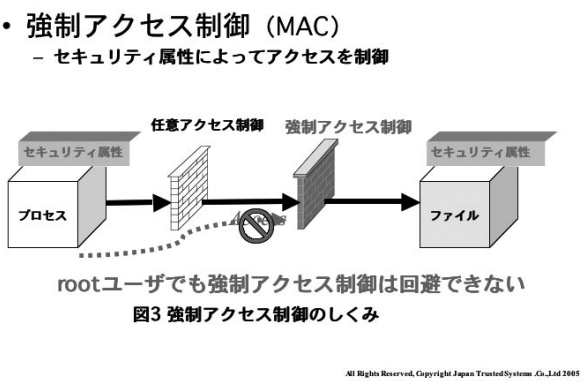

図3 強制アクセス制御のしくみ

この構造の仕組みでは、もしシステム管理者権限を保持したプロセスが悪意を持ったユーザに奪取されたり、システム管理者のパスワードが漏れてなりすまされてログインされたり、あるいはシステム管理者自身が情報を盗み見るために悪意を持ってアクセスした場合など、システムに存在する全ての情報へのアクセス許可を悪意あるユーザに与えたことと同じ状態になります。これではたくさんの時間をかけてセキュリティ設定を正しく行っていたとしても、セキュリティ機能を無効にされたり、ログを削除されるなどして痕跡を消すことができるため、いくら適切にアクセス権を設定してもまったく意味がないのです。一方、TCSEC で定義されている強制アクセス制御は、システム管理者であってもあらかじめ決められた動作以外は行えないようにする機能です。これは、システムに存在するすべてのプロセスやファイルにセキュリティ属性を付与します。この属性はセキュア OS や、トラステッド OS で追加された、これまでの OS にはない属性です。この属性をプロセスがファイルにアクセスするときは必ずセキュリティ属性のチェック機構（リファレンスモニタと呼ぶ）を通過しなければなりません。付与されたセキュリティ属性を識別して、プロセスからファイルへのアクセス可否を判断しています。つまり、強制アクセス制御はシステム管理者であっても決して回避することはできないのです。（図 3）

この仕組みを導入することによって OS そのものがとても強靭になるため、あらゆる攻撃からの耐性を OS 自身に持たせることができます。つまり、現状の OS の問題点であるアクセス制御の弱点や、現在のセキュリティ対策の問題点、パッチマネージメントの問題点をすべて解決することができるのです。

6. セキュア OS は標準の機能へ

セキュア OS やトラステッド OS に実装されている機能は、今後のセキュリティ対策に必要とされ、あたりまえの機能になっていくでしょう。そのため、最近では OS に標準の機能としてセキュア OS を取り組む動きが活発になってきています。セキュア OS をこれまでのセキュリティ対策と組み合わせて使用すれば、ほとんどの問題点を解決し、いままでとは比較にならないセキュリティ強度の高いシステムを構築することができるでしょう。