SAAJ
第 89 回月例研究会
講演記録

№４７　石島　隆

テーマ：「Ｔｒｕｓｔｅｄ　ＯＳによるセキュリティ強化」
講　師：株式会社ＣＲＣソリューションズ
インターネット事業部ネットワークソリューション部
プリンシパルコンサルタント　藤　俊満（トウ　トシミツ）氏
日　時：平成 14 年 7 月 17 日（水）18:30～20:30
場　所：東京労働スクエア（ワーカーズサポートセンター）701 号室
出席者：３６名

本講演においては、まず、情報セキュリティ被害の現状とその特徴について説明され、その対応策としての「Ｔｒｕｓｔｅｄ　ＯＳ」の定義、機能とこれを用いたセキュリティ強化策について、事例を交えた解説があった。

Ⅰ．情報セキュリティの現状と動向

情報セキュリティの現状については、ＩＰＡセキュリティセンターが発表した報告書によると次のとおりである。

1. **攻撃の手口……最も多かったのは、侵入行為に係わる攻撃であり、セキュリティホールへの攻撃やパスワードの奪取による権限の不正取得である。**
2. **攻撃の対象……攻撃対象は、メールサーバー、Ｗｅｂサーバーといったインターネット上からアクセス可能なサーバー類に集中している。**
3. **被害の原因……攻撃の原因として最も多かったのは、古いバージョンの利用やパッチ未導入といったセキュリティ運用面での不備であり、現場において日々のセキュリティ運用が追いついていない現状を示している。**
4. **情報セキュリティに対する不安……ユーザへのアンケートでは、「ネットワークへの無断侵入」への不安が半数を超えており、情報の漏洩や改ざん・破壊についての不安が続き、ネットワーク経由での不正に対する不安が大きい。**
5. **情報セキュリティ対策の問題点……対策については、いくらかけてどこまでやればよいのかがわからないという回答が多く、ユーザは評価指標を求めている。また、開発運用要員の不足や技術・知識不足も挙がっており、対策に十分なリソースを投入できない現状を表している。**

また、公開用Ｗｅｂサーバーへの通信は遮断できず、公開用の通信プロトコル（HTTP）での攻撃が増えてきており、ファイアウォールだけでは保護すべきデータを守れなくなっている。

ＷｅｂサーバーやＷｅｂアプリケーションに多数のセキュリティホールがあり、日々発見されている。ユーザはその影響度を分析し、検証した上で更新作業を行う必要があるが、実際には追いついていないことも多い。

一方、セキュリティマネジメントにおいては、ＢＳ７７９９をベースとして、世界標準（ＩＳＯ１７７９９）が成立し、日本国内においても「情報システム安全対策基準」の後継として、同様にＩＳＯ１７７９９をベースとしたＩＳＭＳが策定されてきており、７７９９系が標準として普及することが予想される。

この７７９９系の標準は、セキュリティポリシーとセキュリティスタンダードまでを規定しているセキュリティマネジメントの標準であるが、具体的な技術面の設定や運用手順までは規定していない。当然、セキュリティマネジメントは必要であるが、ＴｒｕｓｔｅｄＯＳのような具体的なソリューションと組み合わせることが必要である。

Ⅱ．Ｔｒｕｓｔｅｄ　ＯＳのご紹介

１．Ｔｒｕｓｔｅｄ　ＯＳとは？

一般的に、ＴＣＳＥＣ（Trusted Computer Systems Evaluation Criteria）においてレベルＢ以上の条件を満たすオペレーティングシステムをＴｒｕｓｔｅｄ　ＯＳと呼ぶことが多いが、明確な定義がされているわけではない。本講演では、このＴＣＳＥＣのレベル分けによる定義を用いている。

ＴＣＳＥＣは、米国国防総省が軍用のコンピュータシステムを調達するために規定した調達の規格であり、セキュリティ方針（Security Policy）、認証・監査（Accountability）、保証（Assurance）及び文書化（Documentation）の４つのカテゴリーから構成されている。

民間においてもこの規格は利用されており、例えばＯＳのセキュリティレベルを表す場合の基準として使用されたり、ＩＳＯ／ＩＥＣ１５４０８の策定のベースの一つにもなっている。

Ａレベル（セキュリティが高い）からＤレベル（セキュリティが低い）にまで分かれており、一般的なＯＳはＣレベル以下に分類される。

Ｄレベルは、セキュリティのないレベルであり、全てのファイルを見ることができる。ＤＯＳ、Ｗｉｎｄｏｗｓ９５／９８、ＭＡＣ　ＯＳ等がこれに該当する。

Ｃレベルは、任意アクセス制御、ログイン・ユーザ認証及び監査の機能により、ファイルの所有者がコントロールするレベルであり、標準ＵＮＩＸ、Ｗｉｎｄｏｗｓ　ＮＴ等がこれに該当する。

Ｂレベルは、Ｃレベルに加えて、強制アクセス制御、最小特権の機能により、システムが強制的にコントロールするレベルであり、Ｔｒｕｓｔｅｄ　ＯＳは、Ｂレベル以上のＯＳである。

２．Ｔｒｕｓｔｅｄ　ＯＳの機能

Ｔｒｕｓｔｅｄ　ＯＳの機能には、次のようなものがある。

① コンパートメント……ユーザを特定のコンパートメント（部屋）に押し込めてしまうことで権限を限定する機能であり、特定のコンパートメントに所属するユーザは、その他のコンパートメントから排除することが可能である。

② 機密区分（Classification）……TOP SECRET／SECRET／CONFIDENCIAL 等のセキュリティのレベルを示す機能である。

③ 機密ラベル……システムのあらゆる個所（ディレクトリ、ファイル、デバイス、通信データ、プロセス）に、幅広くかつきめ細かくアクセス制御を設定することで、不要なアクセスを防御する機能である。
④ 強制アクセス制御……前述の機密区分とコンパートメントを用いることで、許可されたコンパートメントに対して、許可された権限の範囲内でしかアクセスできないように強制する機能である。
⑤ 最小特権……Ｒｏｏｔのような強大な特権を排除し、特権を 50 から 80 に細分化する機能であり、必要に応じてプロセス単位に特権を付与する。特権の引継は別途定義することにより、プロセスを乗っ取り、子プロセスで何かを実行したくても不可となる。また、たとえＲｏｏｔであっても、定義されていなければアクセス不可となる。

Ⅲ. Ｔｒｕｓｔｅｄ　ＯＳによるセキュリティ強化

１．Ｔｒｕｓｔｅｄ　ＯＳ導入のメリット

Ｔｒｕｓｔｅｄ　ＯＳ導入のメリットには、次のような事項がある。
① 高セキュリティレベルの実現……公的な評価基準であるＴＣＳＥＣで一般のＯＳよりも高度なセキュリティレベルであると認定されたＴｒｕｓｔｅｄ　ＯＳを使用することで、公的に高セキュリティであると評価される。また、100%脆弱性がないとは言い切れないが、今までのところ本来の機能では脆弱性は発見されていない。さらに、公開ハッキングテストでの防御実績（ファイアウォール、ＩＤＳなしの環境で４種類のサーバーを 17 日間防御。アカウントを公開し、540 万件のアタックと４万件以上のログインを受けたがダウンしなかった。）がある。
② 被害の極小化……強制アクセス制御と最小特権により、万が一攻撃されて侵入されても、被害を局所化し、踏み台にされたり、他のサービスに影響を及ぼさないようにできる。
③ サーバーの統合（副次的メリット）……Ｔｒｕｓｔｅｄ　ＯＳのコンパートメント機能を用いることで、複数のサーバーを１台に統合することが可能となる。

Ｔｒｕｓｔｅｄ　ＯＳを導入すれば、全ての問題が解決するわけではないが、Ⅰで述べたＩＰＡセキュリティセンターの調査で挙げられた「⑤情報セキュリティ対策の問題点」に、上記①及び②のような解決策を提供することができる。

２．Ｔｒｕｓｔｅｄ　ＯＳが対象とする市場

Ｔｒｕｓｔｅｄ　ＯＳは全てのインターネット関連ビジネスを対象としているが、金融業界、官公庁、インターネットプロバイダ、認証サービスのユーザが多い。オンライン・バンキング（Credit Suisse）、認証サービス（Identrus CA）、インターネット情報公開（某公益法人）、ホスティング・サービス（ＩＳＰ）の事例の紹介があった。

３．まとめ

国内におけるセキュリティ被害の多くは、インターネット経由での侵入攻撃であり、その原因は運用面での対応が不十分であることに起因している。

ユーザ側での対策の問題点としては、対策にいくらかけてどこまでやればよいのかという指標がないことと、運用面に十分なリソースを投入できないことが指摘されている。

Ｔｒｕｓｔｅｄ　ＯＳは、米国国防総省ＴＣＳＥＣでＢレベル以上の条件を満たすＯＳであり、強制アクセス制御と最小特権機能により被害を極小化し、運用面での負荷を最小限に抑えることが可能である。

しかし、Ｔｒｕｓｔｅｄ　ＯＳだけでは、アプリケーション・通信面や物理・環境面での脆弱性は克服できず、他の対策と組み合わせて実施することが必要である。

（Ｑ＆Ａ）

① 導入・運用コストはどうか？……インプリメンテーションに手数がかかるため、初期導入コストは高いが、人件費を中心とした運用コストは低減される。
② Ｗｉｎｄｏｗｓ　ＮＴのＴｒｕｓｔｅｄ　ＯＳ製品はあるか？……ない。
③ 基本ＯＳのパッチへの対応はどうか？……Ｔｒｕｓｔｅｄ　ＯＳは、基本ＯＳの核の部分を書き換えている。パッチの内容によって個別対応することになる。
④ 機密区分及びコンパートメントの設定には、手数がかかるのではないか？……これらの設定の基本（テンプレート）となるものはあり、本来は、ＩＳＭＳの導入とあわせてやることが望ましい。

（参考資料）Ｔｒｕｓｔｅｄ　ＯＳ製品

① Ｐｉｔ　Ｂｕｌｌ（米国アーガス社製）……サンマイクロシステムズ社からソースコードライセンスを入手し、Ｔｒｕｓｔｅｄ機能を付加したＯＳ。Ｓｏｌａｒｉｓ、ＡＩＸ、Ｌｉｎｕｘで稼働。
② Ｔｒｕｓｔｅｄ　Ｓｏｌａｒｉｓ（米国サンマイクロシステムズ社製）……国防総省向けに出荷されており、基本的に日本国内の一般企業には販売されていない。
③ Ｖｉｒｔｕａｌ　Ｖａｕｌｔ（米国ヒューレットパッカード社製）……商用に販売されており、Ｗｅｂサーバーに特化した製品構造となっている。
④ ＨＰ　Ｓｅｃｕｒｅ　Ｌｉｎｕｘ（米国ヒューレットパッカード社製）……Ｖｉｒｔｕａｌ　Ｖａｕｌｔの技術をＬｉｎｕｘで実現した製品であり、Ｖｉｒｔｕａｌ　Ｖａｕｌｔの廉価版の位置付け。

（感想）

不正アクセスの防御策として、ＯＳレベルでの対策は、効果が高いと考えられ、大変興味深い講演であった。技術面（Ｔｒｕｓｔｅｄ　ＯＳを含む）と管理面（ＩＳＭＳ）を組み合わせて、防御策の有効性を高める必要性を感じた。

以　上