BYOD に対応した IT 資産管理システムの開発

16T253　西岡大助　（最所研究室）

近年，大学や企業で BYOD の使用が増加している．また，ソフトウェアに存在する脆弱性を利用した攻撃も深刻な問題となっており，組織所有の機器のみでなく持ち込み機器に関しても IT 資産管理を行うことが重要な課題となっている．本研究では，持ち込み機器を含んだ組織のネットワークを利用する機器の情報をデータベース化し，一元管理するシステムの開発を行う．

1　はじめに

大学や企業では，個人の端末を持ち込み組織のネットワークに接続して使用することが多い．その際，個人の端末で顧客情報や成績情報といった重要な情報を扱うこともあり，そのような情報を守る必要がある．本大学の持ち込み機器に対する機器管理は，ユーザ情報と MAC アドレスを紐付けて管理するだけとなっており，機器内のソフトウェアが安全なものかわからないため，セキュリティ面で不十分であると考える．

近年ゼロデイ攻撃による被害が深刻なものとなっている．ゼロデイ攻撃とは，ソフトウェアの脆弱性情報が公開されてから，パッチが配布されるまでの間に行われる攻撃のことである．大学のネットワーク内に脆弱性を持つ機器が存在した場合，その脆弱性を利用してその機器だけでなく内部ネットワークに接続されている機器全てが攻撃されてしまう恐れがある．

そこで本研究室では，楠目，竹原と共同で脆弱性情報に基づいたセキュリティ対策システムの研究を行っている．公開された脆弱性情報と機器にインストールされているソフトウェアの情報を照らし合わせることで，その脆弱性の影響範囲と対策を算出する．その結果から，脆弱性を持つ機器のネットワーク制御を行うことで内部ネットワークのセキュリティを向上させる．

本研究では IT 資産を管理する機構の開発を行う．組織のネットワークに接続されている機器の情報とユーザ情報を紐付けてデータベース化し，一元管理することでユーザの持つ機器の情報取得を容易にする．本稿では，IT 資産を管理するデータベースの設計と，Linux を対象としたソフトウェア情報を取得するためのエージェントについて述べる．

2　セキュリティ対策システム

セキュリティ対策システムの概要を図 1 に示す．このシステムは，IT 資産管理部，脆弱性情報収集部，影響算出部，ネットワーク制御部の 4 つで構成されている．

IT 資産管理部は，本研究の対象である．持ち込み機器を含む，組織のネットワークに接続された機器の情報をデータベース化して一元管理する．現時点で管理する情報としては，機器の所有者，MAC アドレス，固定 IP アドレス，OS 情報，機器の重要度，インストールされているソフトウェアの情報などがある．

脆弱性情報収集部は，同研究室の楠目によって開発されている．公開された脆弱性情報を掲載している JVN から，脆弱性情報を取得しデータベース化する．脆弱性情報には，脆弱性の内容，ソフトウェア名，製品名，ベンダ情報，脆弱性の発見日，脆弱性の深刻度，パッチの有無が含まれている．

影響算出部では，IT 資産情報と脆弱性情報を照らし合わせ，組織内の機器の脆弱性を調べる．脆弱性が存在した場合，機器の所有者に通知する．脆弱性の深刻度と IT 資産情報の重要度を基に，実際にネットワークから遮断するかどうかの判断も行う．

ネットワーク制御部は，同研究室の竹原によって開発されている．影響算出部の指示に基づいてネットワークの制御を行う．ネットワーク制御は，Firewall を用いた外部ネットワークからの遮断と，L2 スイッチを用いた内部ネットワークからの遮断の 2 段階の流れで行われる．

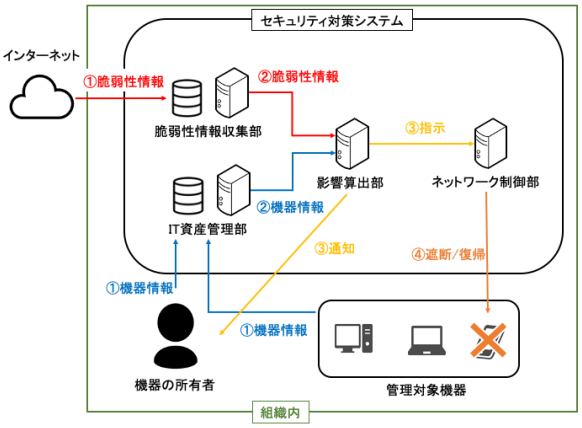

図 1: セキュリティ対策システム概要

3　IT 資産管理システム

3.1　概要

IT 資産管理システムの概要を図 2 に示す．MAC アドレス，固定 IP アドレス，OS 情報，重要度といった情報は機器の所有者によってブラウザから登録させる．ソフトウェア情報の取得はエージェントを用いて行う．本システムは香川大学の情報セキュリティポリシに基づいて開発を行う．

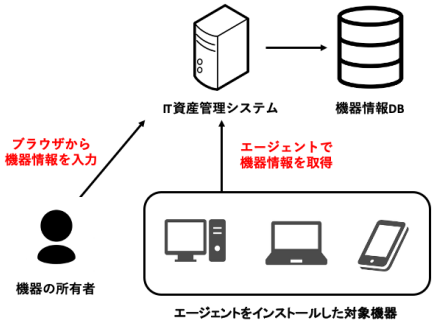

図 2: IT 資産管理システム概要

3.2　情報取得の流れ

IT 資産情報取得の流れについて述べる．まず，内部ネットワークに接続したユーザは，Web ブラウザを用いてログイン認証を行う．その後ハードウェア情報として，MAC アドレス，固定 IP アドレス，OS 情報，機器の重要度を登録する．ユーザの負担を軽減するため，MAC アドレスと OS 情報は自動取得する．機器の重要度の決め方は，その機器に求められる可用性や保存される情報の種類をアンケート調査する方法などを検討している．次に，ソフトウェア情報を取得するためのエージェントをインストールする．最後に，エージェントを用いてソフトウェア情報の取得を行う．

3.3　IT 資産管理データベース

IT 資産情報を管理するためのデータベースを ER 図で表したものを図 3 に示す．IT 資産管理データベースは，ユーザテーブル，ステータステーブル，ハードウェアテーブル，ソフトウェアテーブル，OS テーブルから構成される．緑色のエンティティはユーザ情報，赤色のエンティティは機器情報を表している．

3.4　エージェントを用いた情報取得

エージェントでは，機器にインストールされているソフトウェアの名前とバージョンを取得する．本稿では，Linux に対応した実装について述べる．Linux はインストールされているソフトウェアがパッケージ管理されているため，パッケージの一覧を取得するコマンドにより，ソフトウェア情報を取得する．情報の送受信には HTTP を用いる．ソフトウェア情報は，機器の OS によって取得できる形式が異なるため，サーバへ送信する際 JSON 形式に成形して送信する．そのため，エージェントには取得したソフトウェア情報を，JSON 形式に変換する機能が必要になる．エージェントプログラムは管理対象となる機器の OS 毎に実行可能なコードを生成する必要があるため，クロスコンパイルに対応している Golang を用いて実装を行う．

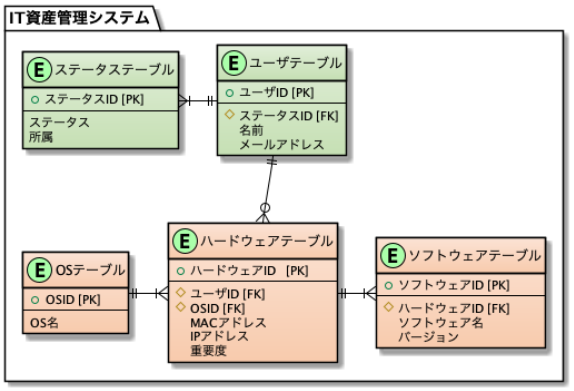

図 3: ER 図

実装したエージェントの機能テストの手順について述べる．まず，機器情報を受け取るためのサーバを起動する．次にクライアント上でエージェントを実行しソフトウェア情報を取得する．取得した情報をサーバへ送信する．最後にサーバ側で受け取った情報をデータベースに格納する．

上記の手順実行後のソフトウェアテーブルの内容を図 4 に示す．図中の左側が，Linux コマンドで表示したソフトウェア情報，右側がソフトウェアテーブルの内容となっている．赤枠がソフトウェア名，青枠がバージョンとなっており，設計通りのデータが取得できていることが確認できる．

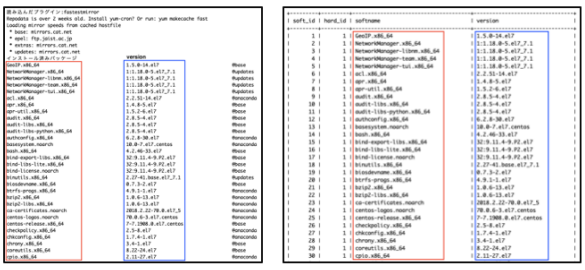

図 4: ソフトウェア情報取得結果