脆弱性情報を用いたセキュリティ保護システム“BEYOND”の開発

中村 友昭 [1)], 竹原 一駿, 大野 真伯, 山下 俊昭, 宗雪 勝也,
小野 滋己, 喜田 弘司, 後藤田 中, 最所 圭三

香川大学

1) s22g359@kagawa-u.ac.jp

Development of Security Protection System “BEYOND” Using Vulnerability Information

Tomoaki Nakamura, Ichitoshi Takehara, Masanori Ono, Toshiaki Yamashita,
Katsuya Muneyuki, Shigemi Ono, Koji Kida, Naka Gotoda, Keizo Saisho

Kagawa Univ.

概要

近年，脆弱性を利用した攻撃が増加しており，こうした攻撃は標的型攻撃と組み合わせることで被害は甚大なものになる．また，大学や企業において BYOD が増加しておりこうした機器の管理は機器の所有者に一任することが多く脆弱性があるにも関わらず対応していない事が多い．そこで，本研究では，組織内の機器に対していち早く脆弱性への対応を誘導し，脆弱性を用いた攻撃を防ぐことで組織の情報資産を保護するシステム “BEYOND”(Bring Enhancement Your Own Non-Vulnerable Device) の開発を行っている．本稿では，“BEYOND” の開発及び “BEYOND” を本学の情報メディアセンターで運用に向けたシステムの有効性の検証を行った．検証の結果，現状のシステムでは BYOD に対して適用することは難しいことがわかった．しかし，検証によって新たに要件を見つけることができたため，それらに対応することで BYOD にも対応できると考えられる．

1 はじめに

近年，脆弱性を利用した攻撃が増加しており，被害が深刻化している．例えば，Windows のファイル共有 (SMB1.0) の脆弱性を利用したランサムウェア WannaCry [1] は，脆弱性を持つ機器に感染し，それを起点として機器が接続している LAN 上にある同種の脆弱性を持つ機器に感染を繰り返す．このような攻撃による被害を防ぐためには，脆弱性をいち早く検知して無くすことが重要である．

一方，大学や企業などの組織では，個人で所有する機器を持ち込み，組織のネットワークに接続し，業務に使用する BYOD (Bring Your Own Device) が増加しており，個人の機器に成績情報や顧客情報などの情報資産を保存することがある．香川大学でも BYOD を導入しており，多くの教職員や学生が個人機器を利用している．しかし，こうした機器は機器の所有者が手間を理由にソフトウェアの更新を怠っていることや脆弱性があることを認識していないなど，管理は不十分な場合が多い．

そこで我々は，組織内の機器に対していち早く脆弱性への対応を誘導し，脆弱性を用いた攻撃を防ぐことで組織の情報資産を保護するシステム “BEYOND”(Bring Enhancement Your Own Non-Vulnerable Device) の開発している [2].

本稿では，“BEYOND” の開発について述べるとともに，香川大学の情報メディアセンター [3] にて運用中のサービスに本システムを仮導入した上での有効性の検証について述べる．

2 香川大学における脆弱性対策

2.1 現状と課題

香川大学で用いられている機器の現状について以下に示す．

基盤サーバ

情報メディアセンターなどが運用する学生や教職員向けにサービスを提供するサーバである．学生の個人情報や学習管理システム (LMS) などが運用されている．一部の機器は専門の外部業者に運用を委託している．

研究サーバ

研究室にて教員 (所有者) の管理下にて運用されているサーバであり，その教員が担当する講義資料の公開や研究に用いられる．所有者は，固定 IP アドレスの登録や DNS の登録には OS 情報や利用目的等を情報メディアセンターに申請する必要がある．

個人機器

学生や教職員 (所有者) の持ち込み機器であり，ノート PC やスマートフォンがある．所有者は，初回持ち込み時に MAC アドレス等を情報メディアセンターに申請し，登録されることで学内ネットワークへの接続が許可される．学内ネットワークを経由して学外ネットワークへのアクセスが可能であるが，外部ネットワークからのアクセスは不可能である．

上述した中で特に基盤サーバに対しては特に脆弱性対策を行う必要があると考えた．

2.2 基盤サーバに求められる要件

2.2.1 最新の脆弱性情報の収集

CSIRT は常時最新の脆弱性の深刻度などの情報 (脆弱性情報) を収集，管理する必要がある．脆弱性が公開されてからベンダーからのパッチが配布される前であったり，公開されていないが SNS 上の噂レベルで広まっている脆弱性を利用した攻撃を受ける可能性がある．また，注意喚起や組織内での公開のために，機器の情報とマッチングしやすい形式に整形して管理する．

2.2.2 組織にある機器情報の収集

組織内のネットワークを利用する機器について，設置機器と持ち込み機器の区別なく，機器にインストールされているソフトウェアとバージョン，利用実態などを収集し，機器の所有者と紐付けて一元管理する必要がある．ソフトウェアは，所有者が利用しながらバージョンを更新することが考えられるため，機器情報を継続的に収集することが求められる．脆弱性を持つ機器をネットワーク上で特定するために，MAC アドレスや IP アドレスが必要である．脆弱性情報と同様にマッチングしやすい形式に整形して管理する．

2.2.3 脆弱性を持つ機器の特定

2.2.1 項，2.2.2 項にて収集した脆弱性情報と機器情報を用いて，利用者にとって重要な注意を喚起するため，脆弱性を持つ機器を特定する必要がある．脆弱性はソフトウェアの特定のバージョンや，特定の OS で動くソフトウェアにのみ存在する事が多い．そこで，脆弱性の検出にはソフトウェア名だけでなくバージョンや実行環境を考慮する．

2.2.4 利用実態をもとにした脆弱性への方針算出

脆弱性の深刻度によるリスクと，機器の利用実態から脆弱性対策とその方針を算出し，通知することが必要である．発見された脆弱性の深刻度が高い場合は即座にサービスを停止し，脆弱性に対応をすることが望ましいが，発見された脆弱性の深刻度が低い場合や特定の期間中はサービスを停止できない場合はサービスの継続を優先する選択も考えられる．特定の期間中にサービスが停止できないと場合には，香川大学の場合，試験期間中の成績処理サーバやオープンキャンパス期間中の大学の Web サイトがあげられる．そのため，脆弱性の深刻度だけでなくサービスの利用実態に基づいた対策が求められる．

2.2.5 脆弱性を持つ機器に対してのアクセス制御

算出された制御方針として，外部ネットワークとのアクセスのみを遮断することが考えられる．例えば，試験期間中の成績処理サーバが脆弱性をもった場合は，外部ネットワークを遮断し学内からのみ利用可能にするといった場合が考えられる．脆弱性を持つ機器をネットワーク上で特定する識別子として MAC アドレスや IP アドレスを用いて，脆弱性が修正されるまで一時的に，機器や動作するサービスのアクセスの制御が求められる．

以上の要件を BEYOND では解決することを目指す．

3 “BEYOND” の開発

BEYOND は脆弱性情報収集部 [4]，IT 資産管理部 [5]，影響算出部 [6]，ネットワーク制御部 [7] で構成される (図 1)．

BEYOND の各機構の役割について述べる．脆弱性情報収集部は，脆弱性情報公開サイトから最新の脆弱

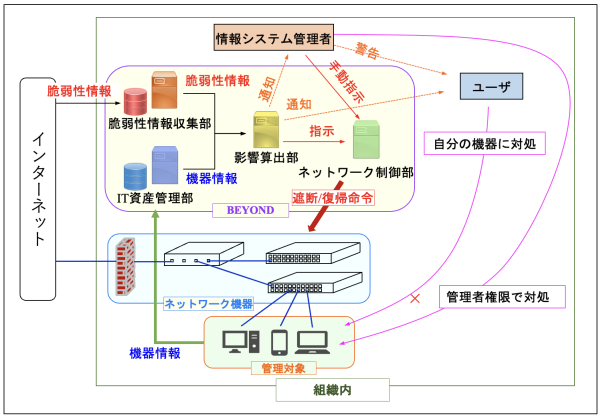

図 1 BEYOND の全体構成

性情報を収集し，影響算出部で扱いやすい形に整形して DB に登録することで 2.2.1 項を解決する．IT 資産管理部は組織のネットワークを扱う機器の情報を収集し，影響算出部で扱いやすい形に整形して DB に登録する 2.2.2 項を解決する．影響算出部は脆弱性情報収集部と IT 資産管理部で収集したデータを用いて，組織内の機器に存在する脆弱性を検知し，対策方針を算出し通知することで要件 2.2.3 項，2.2.4 項を解決する．ネットワーク制御部は影響算出部の対策方針に基づいて脆弱性を持つ機器のアクセス制御を行うことで要件 2.2.5 を解決する．

以下に各機構の機能を示す．

3.1 脆弱性情報収集部

本機構はインターネット上に公開されている脆弱性情報を収集し，独自に設計した DB に登録して管理することで，脆弱性の検知や対策を取れるようにすることを目的としている．本機構において前項の 2.2.1 項を解決するための機能について以下に示す．

3.1.1 脆弱性情報の管理

脆弱性情報を収集するための情報源は主に JVN (Japan Vulnerability Notes) [8] と NVD (National Vulnerability Datavase) [9] を用いている．JVN は日本で使用されているソフトウェアを対象に脆弱性関連情報と対策情報を提供し情報セキュリティ対策に資することを目的とする脆弱性対策ポータルサイトであり，NVD とは CVE(共通脆弱性識別子) [10] と同期した脆弱性データベースのことである．本機構で収集している脆弱性情報のうち，脆弱性の検出や対策方針の算出に用いるものを表 1 に示す．このうち，脆弱性の検出には表 1:versions が使われる．脆弱性を持つ製品の種別 (ハードウェア，OS，ソフトウェア等) とベンダ名，製品名をまとめた CPE やどのバージョン間に脆弱性が存在するかという情報，どの OS 上で動作するかという情報をまとめて管理している．ここでソフトウェア名と脆弱性を持つバージョンの範囲が正確に収集できていない場合，検知漏れや誤検知が起きる可能性がある．脆弱性の対策には表 1:CVSS が用いられる．CVSS [11] は脆弱性の深刻度を表すもので，これはベンダに依存せず，同一の基準のもとで脆弱性を評価した値である．0.0〜10.0 までの範囲で表され，値が大きいほど深刻度が高いと判断される．現在，影響算出部ではこの値に閾値を設定して，対策方針を算出している．

3.1.2 最新の脆弱性情報の収集

現在，過去の脆弱性情報は年ごとの脆弱性情報をまとめたデータフィードから取得している．しかし，最新の脆弱性情報はデータフィードに掲載されるまで時間がかかるため日付指定で直近の脆弱性情報を収集している．新規の脆弱性情報はそのまま登録し，変更のあった脆弱性情報は登録されている情報の更新を行っている．これらの処理を時間指定で定期的に行うことで常に最新の情報を保っている．

3.1.3 収集した脆弱性情報の整形処理

脆弱性を持つ製品のバージョン情報の範囲はバージョンの開始位置と終了位置にそれぞれ含む場合と含まない場合がある．そのため，検知を行う製品のバージョンが脆弱性を持つ範囲の境界にある場合これらの場合分けができないと検知漏れを起こす場合がある．そのため，バージョンの開始位置，終了位置の含む場合と含まない場合の組み合わせをそれぞれパターン分けしておくことで，影響算出部で検知する際の検知漏れを無くせるようにしている．また，CPE 情報は JVN と NVD で表記方法が異なる．そのため，これらの情報は JVN に合わせる形で整形処理を行っている．

3.2 IT 資産管理部

本機構は組織のネットワークを利用する全ての機器の情報を収集し一元管理することで，必要な情報を迅速に提供することを目的としている．情報の収集には Web ブラウザからの入力とソフトウェアエージェントを用いて行う．本機構において前項の 2.2.2 項を解決するための機能について以下に示す．

3.2.1 アクセス制御のための情報収集

機器本体の情報は Web ブラウザからの入力で実現する (表 2:Hardware)．登録する機器には，組織のセキュリティポリシに基づいた重要度をつけ，利用者のユーザ ID と紐付けて管理する．重要度をつけて管理することで，その値に沿って保護の優先度を変えるなど，柔軟な対策を取ることが可能になる．脆弱性の中には特定の OS のみに存在するものもあるため，OS を管理することでそのような脆弱性を正しく検出できるようにする．MAC アドレス，固定 IP アドレスは機器を識別したり，ネットワーク制御部でアクセスを制御する際に用いる．

表 1　脆弱性情報収集部で管理している情報

管理する情報	詳細
versions	脆弱性の識別子，CPE，脆弱性を持つバージョンの範囲，OS
CVSS	CVSS スコア，深刻度

3.2.2 機器にインストールされているソフトウェア情報の収集

機器にインストールされているソフトウェア情報はエージェントを用いて取得することで実現する (表 2:Software)．機器内のソフトウェアは非常に数が多く，ユーザがソフトウェアをインストールした際に，依存関係にあるソフトウェアが自動でインストールされる場合もあり，ユーザが自ら全ての情報を登録することは不可能である．そこで，エージェントを用いて自動で情報を取得することで全ての情報を漏れなく登録する．現在エージェントは Windows，Ubuntu 系 OS，Debian 系 OS に対応しており，ソフトウェア名とバージョン番号はパッケージ管理ソフトウェアから収集している．パッケージ管理ソフトウェアの形式等の変化によりソフトウェア名とバージョン番号が収集できない場合や想定している方法で管理できない場合，検知漏れや誤検知が起きる可能性がある．

3.2.3 機器の利用実態の収集

機器の利用実態を収集するにあたって，漏れなく情報を収集するために，機器の所有者に情報登録を強制させることが重要になる．そこで，サービス提供に利用する IP アドレスとポート番号を登録させ，ネットワーク制御部と連携して，その IP アドレスとポートでの通信を許可することで，全てのサービス情報の管理を実現する．管理する情報は表 2:Service の通りである．サービスの提供範囲は内部限定，外部公開が考えられ，提供範囲に応じたアクセス制御方針を算出可能にする．機器の停止可能期間はいつでも停止可能な場合や，時間や曜日を指定して停止可能などが考えられる．その情報から，停止できる場合はアクセス制御を行ったり，停止可能期間にアップデートを促すなどの対策が可能になる．

3.3 影響算出部

本機構は脆弱性情報収集部と IT 資産管理部で管理されている情報を突き合わせることで脆弱性を検知する．検知した脆弱性の深刻度と機器の利用実態からアクセス制御ポリシーを算出する，本機構において前項の 2.2.3 項と 2.2.4 項を解決するための機能について以下に示す．

表 2　IT 資産管理部で管理している情報

管理する情報	詳細
Hardware	MAC アドレス，固定 IP アドレス，OS，重要度
Software	ソフトウェア名，バージョン番号
Service	使用しているソフトウェア，提供範囲，停止可能期間，IP アドレス，ポート

3.3.1 脆弱性の検知

脆弱性情報収集部 DB 及び IT 資産管理 DB から，それぞれソフトウェア名とバージョン情報を取得する．取得したソフトウェア名とバージョン情報のパターンマッチングを行い，脆弱性を含むソフトウェアを探し出す．脆弱性を含むソフトウェアをインストールしている機器を特定して，アクセス制御ポリシーを決定する．

3.3.2 機器の利用実態に基づいたアクセス制御ポリシーの決定

脆弱性の深刻度が高いものは重大なインシデントを引き起こす可能性や，単純な操作で攻撃を行う事ができる可能性が高く，被害が甚大になることが想定される．攻撃による被害を防止するために，早急にアップデートしたり，アクセス制御を行うなどして，攻撃のリスクを下げなければならない．しかし，何らかのサービスを提供しているサーバなどの場合は，一律的なアクセス制御を行うことができない．そこで，アクセス制御ポリシーを決定する指標として，脆弱性の深刻度を表す CVSS スコアと，機器の利用実態を利用する．CVSS スコアを用いたアクセス制御ポリシーの決定のための閾値として 4.0 以上の脆弱性に対して対応を行う．閾値の決定理由として PCI-DSS [12] では，CVSS スコアが 4.0 以上の脆弱性を不合格と判断しているため，これを参考にした．表 3 に考案したアクセス制御ポリシーの一例を示す．表 3:パターン a は，サービスが外部に公開されている場合の対処法である．これにより，外部から攻撃を防ぐことができる．表 3:パターン b は，外部からアクセスすることができ，内部に向けたサービスを提供している場合の対処法であり，内部ネットワークに接続された機器にすでに攻撃 Bot がいる可能性や，該当機器がすでに脆弱性を利用した攻撃を受けておりマルウェアなどを保持している可能性があるときに有効である．表 3:パターン c では，表 3:パターン a と表 3:パターン b の両方を防ぐことができる．

表 3　アクセス制御ポリシーのパターン

パターン	制御ポリシー
a	外部との通信を遮断する
b	内部との通信から隔離する
c	外部と内部の通信を両方切断する
d	何もしない

3.4　ネットワーク制御部

影響算出部で算出されたアクセス制御ポリシーをもとに該当機器に対してアクセス制御を行う．該当機器について影響算出部からは，制御ポリシーと MAC アドレスを受け取る．ネットワーク内において，該当機器を含む管理対象機器は Firewall，L2 スイッチに接続されている．本機構において前項の 2.2.5 項を解決するための機能について以下に示す．

3.4.1　外部ネットワークからの遮断

まず，外部との通信を遮断する制御ポリシー (表 3: パターン a) の実現方法を述べる．これは，Firewall を操作することで実現する．影響算出部から受け取った該当機器の MAC アドレスを用いて，IT 資産管理部より，固定 IP アドレスを得る．これにより，該当機器と外部ネットワークとの通信を遮断するルールを生成し，Firewall に適応することで遮断する．外部ネットワークの機器である，“133.92.147.224” と接続できなくなる様子を図 2 に示す．

復帰時には，生成したルールを削除する．

3.4.2　内部ネットワークからの隔離

次に，内部との通信から隔離する制御ポリシー (パターン b) の実現方法を述べる．L2 スイッチを用いて，内部ネットワークから隔離する．該当機器による，内部ネットワークに存在する他の機器への攻撃を防ぐために，L2 スイッチの VLAN の機能を用いて該当機器を検疫ネットワークへ隔離する．L2 スイッチが保持する FDB (Forwarding DataBase) を用い，MAC アドレスより，L2 の接続ポートを取得し，その接続ポートを検疫 VLAN に所属させることで，該当機器を隔離する．復帰時には，該当の接続ポートを検疫 VLAN から内部 VLAN に戻す．

以上の手法で該当機器がネットワークから遮断されたときに，該当機器の所有者は影響算出部からの通知に気づいていない可能性がある．所有者は，ネットワークから遮断されたことを異常と考え，他の L2 スイッチの接続ポートに該当機器を接続し，ネットワークへの再接続を試みる場合がある．そのため，該当機器が常時隔離され続けている状態を維持することが必要である．該当機器の MAC アドレスが，内部に接続されていないか監視を続け，接続されたら再び隔離する．本論での実装では，同一の L2 スイッチの接続ポートの差し替えにのみ，対応する．FDB を監視することで，該当機器が接続しているポートの変更を検知する．変更されたことを検出すると，変更前の接続ポートを内部 VLAN に復帰し，変更後の接続ポートを検疫 VLAN に接続し直す．これにより，該当機器は常に検疫ネットワークに隔離される．図 3 にて接続ポートの変更に追従して，隔離している実行結果を示す．

```
01:  $ ping 133.92.147.224 -c 20
02:  PING 133.92.147.224 (133.92.147.224) 56(84) bytes of data.
03:  64 bytes from 133.92.147.224: icmp_seq=1 ttl=63 time=1.46 ms
04:  64 bytes from 133.92.147.224: icmp_seq=2 ttl=63 time=1.27 ms
05:  64 bytes from 133.92.147.224: icmp_seq=3 ttl=63 time=1.28 ms
06:  64 bytes from 133.92.147.224: icmp_seq=4 ttl=63 time=1.31 ms
07:  64 bytes from 133.92.147.224: icmp_seq=5 ttl=63 time=1.37 ms
08:  64 bytes from 133.92.147.224: icmp_seq=6 ttl=63 time=1.30 ms
09:  64 bytes from 133.92.147.224: icmp_seq=7 ttl=63 time=1.16 ms
10:  64 bytes from 133.92.147.224: icmp_seq=8 ttl=63 time=1.08 ms
11:
12:  --- 133.92.147.224 ping statistics ---
13:  20 packets transmitted, 8 received, 60% packet loss, time 19419ms
14:  rtt min/avg/max/mdev = 1.083/1.285/1.466/0.114 ms
```

8回目以降の通信が遮断

図 2　外部との通信の切断の様子

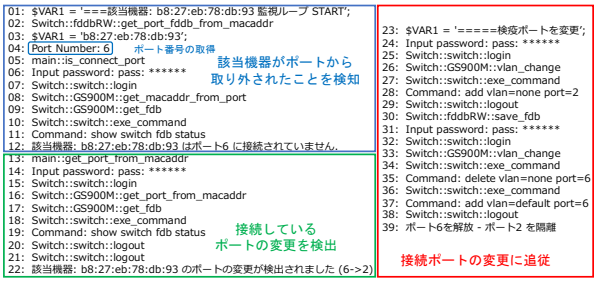

図 3　ポートの監視と追従の実行結果

4　評価

4.1　評価目的

本稿では “BEYOND” の有効性の確認と 2 章以外の新たな要件の調査を目的とした評価実験を行う．これは “BEYOND” 全体を結合させ，一つのシステムとして動作させたときの評価が行われていないためである．評価実験を行う対象として香川大学の学内限定で公開しているサービスを運用しているサーバに対して行う．これは，2.1 節で述べた基盤サーバに該当する．BYOD ではなく基盤サーバを対象とするのは，基盤サーバは BYOD に比べ台数が少なく使用用途が明確であるため BYOD に対して評価を行う前に評価実験を行うべきだと考えたからである．

4.2　評価方法

本評価実験では以下の条件で評価を行った．

脆弱性情報収集部

JVN は 1998 年から 2022 年 10 月 12 日までに収集したもので NVD は 2002 年から 2022 年 10 月 12 日までに収集したものとする．

IT 資産管理部

Web ブラウザとエージェントを用いて機器情報の収集を行う．エージェントでソフトウェア情報を登録するために必要な機器情報は予め入力済みとする．香川大学の学内限定で公開しているサービスを運用しているサーバ 2 つに対してエージェントを導入しソフトウェア情報 (ソフトウェア名及びそのバージョン番号) を収集する．収集できたソフトウェア情報は PC ルームの空き情報管理システムで 28 件，インストーラーのダウンロードシステムで 51 件であった．

以下の流れで評価実験を行う．

- 脆弱性情報 DB と IT 資産管理 DB の両方からソフトウェア名とバージョン情報を取得する．このとき IT 資産管理 DB から取得するソフトウェア情報は本来であればサービスで使用されているソフトウェアのみ取得するが，使用されているソフトウェアが不明瞭なため機器にインストールされているソフトウェア全て取得する．
- 取得したソフトウェア名同士が一致するものを探し，一致したものがあればバージョン情報を比較してソフトウェアが脆弱性を含むバージョンの範囲内であるか確認する．
- 脆弱性を含むソフトウェアが発見された場合，脆弱性の深刻度を脆弱性情報 DB から参照し深刻度の値とサービスの利用形態からアクセス制御ポリシーを決定する．
- 検知された脆弱性情報と手動で調査を行った結果を比較し，検知漏れ，誤検知が無いか調べる (表 4)．

4.3 評価結果

評価結果は表 5 のようになった．

正常検知できた脆弱性について述べる．正常検知できた脆弱性の一つに “VMware_Tools” があった．この脆弱性は表 6 と表 7 に示すように DB に登録されていた．脆弱性情報 DB でのソフトウェア名と IT 資産管理 DB のソフトウェア名が一致しており，IT 資産管理部でソフトウェア名とバージョン番号を正確に取れている場合正確に脆弱性を検知できる．

表 4　脆弱性検知の区分分け

	検知可	検知不可
脆弱性有	正常検知	検知漏れ
脆弱性無	誤検知	

表 5　評価実験の結果

対象機器	インストールされている ソフトウェア	正常検知	検知漏れ	誤検知
PC ルームの管理システム	28 件	2 件	2 件	5 件
インストーラーのダウンロードサイト	51 件	3 件	3 件	8 件

表 6　脆弱性情報 DB

CVE_ID	CPE	バージョン開始位置	バージョン終了位置
CVE-2022-31676	cpe:/a:vmware:tools	11.0.0	12.1.0
CVE-2022-31676	cpe:/a:vmware:tools	10.0.0	10.3.25
CVE-2022-31676	cpe:/a:vmware:tools	10.0.0	12.1.0
CVE-2022-22977	cpe:/a:vmware:tools	10.0.0	10.3.24

表 7　IT 資産管理 DB

ソフトウェア名	バージョン番号
VMware_Tools	10.3.5.10430147

次に検知漏れしたものについて述べる．検知漏れの原因は脆弱性情報収集部での収集ミスと IT 資産管理部でソフトウェア名とバージョン番号が想定通りに取得できていないことであった．検知漏れした脆弱性に “Microsoft_ODBC_Driver” と “OpenSSL” があった．

Microsoft_ODBC_Driver

検知漏れの原因として収集元の情報の不備が考えられる．本ソフトウェアは JVNDB-2022-002407 [13] によると

> 複数の Microsoft Windows 製品には、Microsoft ODBC ドライバに不備があるため、リモートでコードを実行される脆弱性が存在します。

と記述されている．しかし，影響を受けるソフトウェアには ODBC ドライバが無い．また，複数の Microsoft Windows 製品とあるが，該当する製品は機器情報に含まれていなかった．

OpenSSL

検知漏れの原因として機器情報の取得ミスが考えられる．IT 資産管理部のエージェントを用いて取得した時，表 8 に示すように DB に登録されていた．ソフトウェア名の中にバージョン番号が含まれており，ソフトウェア名とバージョン番号を分けて登録できていなかったため本脆弱性を検知することができなかった．表 8 の場合ソフトウェア名末尾の “1.1.1d_(64-bit)” がバージョン番号として取得できていれば検知できていた．

最後に誤検知したものについて述べる．誤検知の原因は影響算出部での検知方法に起因するものであった．誤検知したソフトウェアを表 9 に示す．

表 8　バージョン番号が取れなかった場合の IT 資産管理 DB

ソフトウェア名	バージョン番号
OpenSSL_1.1.1d_(64-bit)	NULL

表 9　誤検知したソフトウェア

ソフトウェア名	バージョン番号
SQL_Server_Management_Studio_for_Reporting_Services	15.0.18206.0
SQL_Server_Management_Studio_for_Analysis_Services	15.0.18206.0
SQL_Server_Management_Studio_for_Analysis_Services_Localization	15.0.18206.0

誤検知の原因としてパターンマッチングを行う際 “SQL_Server_Management_Studio” の部分が脆弱性情報 DB に存在するソフトウェア名と部分一致したためだと考えられる．これは，脆弱性情報 DB で収集しているソフトウェア名と IT 資産管理部で収集しているソフトウェア名に表記揺れがあるためソフトウェア名が完全一致とすると，脆弱性が全く検知できないためである．そのため，脆弱性情報収集部と IT 資産管理部で収集している情報の表記ゆれを無くすことで誤検知の数は減らせると考えられる．

5　おわりに

“BEYOND” は組織内の機器に存在する脆弱性に対してアクセス制御を行うことで脆弱性を利用した攻撃から機器を保護することを目的としている．今回はその前段階として “BEYOND” を用いて，本学の情報メディアセンターで使用している機器内に脆弱性が存在するか評価を行った．評価結果から実際に脆弱性があるソフトウェアの中で半分は正確に検知できていた．また，今回の評価実験で浮き彫りとなった “BEYOND” 各機構の課題を解決することで基盤サーバにおいては本システムを適用して脆弱性対策が行えると考えられる．しかし，今回はネットワーク制御部の評価を行う事はできなかったため，“BEYOND” の目標であるアクセス制御を用いて脆弱性対策を行うということは検証できなかった．さらに，現状の精度では台数が多く，使用用途も多岐に渡る BYOD に対して適用することは難しい．今後は検知の精度を高めて，実際にアクセス制御を行い，BYOD に対して “BEYOND” が有効であるか検討したい．

参考文献

[1] 倪永茂,“ランサムウェア WannaCry の仕組みとその対策”, 宇都宮大学国際学部研究論集 Vol.46, pp79-85, 2018.

[2] 楠目幹, 喜田弘司, 最所圭三、脆弱性情報を利用したゼロデイ攻撃対策システムにおける構成情報収集機能の実装及び脆弱性評価機能の設計、ISEC2019-12、Vol.119、no.140、pp.1-6(2019).

[3] 香川大学情報メディアセンター、https://www.itc.kagawa-u.ac.jp/、2022/10/6.

[4] 中村友昭, 竹原一駿, 西岡大助, 細川洋輪, 岩下連師, 喜田弘司, 最所圭三、脆弱性情報を用いたセキュリティ保護システムにおける脆弱性情報収集部の改善、令和 3 年度電気・電子・情報関係学会四国支部連合大会講演論文集、Vol.2021、pp.178-178(2021).

[5] 西岡大助, 楠目幹, 竹原一駿, 細川洋輔, 喜田弘司, 最所圭三、脆弱性情報を利用したセキュリティ対策支援システムにおけるサービス情報管理のための IT 資産管理機構の開発、第 83 回情報処理学会全国大会講演論文集,Vol.3, pp.419-420(2021).

[6] 細川洋輔, 竹原一駿, 西岡大助, 中村友昭, 岩下蓮師, 喜田弘司, 最所圭三、脆弱性情報を用いたセキュリティ保護システムにおける機器の利用実態に基づいたアクセス制御ポリシーの考案、令和 3 年度 電気・電子・情報関係学会 四国支部連合大会 講演論文集,Vol.2021, pp.177(2021).

[7] 竹原一駿, 楠目幹, 西岡大助, 喜田弘司, 最所圭三、脆弱性情報を用いたセキュリティシステムにおけるネットワーク制御機構に関する研究、令和 2 年度電気・電子・情報関係学会四国支部連合大会論文集,Vol.2020,pp.16-4.

[8] JPCERT/CC and IPA,https://jvn.jp/,2022/10/6.

[9] National Institute of Standards and Technology,urlhttps://nvd.nist.gov/,2022/10/6.

[10] The MITRE Corporation,https://cve.mitre.org/,2022/10/6.

[11] National Institute of Standards and Technology,https://nvd.nist.gov/vuln-metrics/cvss,2022/10/6.

[12] PCI Security Standards Council,https://listings.pcisecuritystandards.org/documents/ASV_Program_Guide_v3.0.pdf,2022/10/6.

[13] JPCERT/CC and IPA,https://jvndb.jvn.jp/ja/contents/2022/JVNDB-2022-002407.html,2022/10/17.