セキュリティの脆弱性評価技術とサイバー攻撃エミュレーション技術

Vulnerability Assessment and Cyberattack Emulation Technologies for Accurate Risk Assessment

青木　慧 AOKI Satoshi　春木　洋美 HARUKI Hiroyoshi　佐藤　俊至 SATO Toshiyuki

サイバー攻撃からシステムを守るには，リスクを評価し，適切な対策を講じなければならない。リスクの評価では，脆弱（ぜいじゃく）性を検査するだけでなく，実際に攻撃を行って標的となるシステムへの影響や攻撃の難易度を評価することも重要である。一方，脆弱性検査の自動化が進む中で，攻撃者視点でのサイバー攻撃への耐性評価は，攻撃ノウハウを持つセキュリティの専門家に依存するという問題がある。

そこで東芝グループは，サイバー攻撃耐性評価を自動で行うサイバー攻撃エミュレーション技術の研究開発を進めている。今回，外部との様々なインターフェースを持つ複合機（MFP：Multifunctional Peripherals）サービスをモチーフに，実際に攻撃までを行う脆弱性評価を専門家が実施した結果を元に，耐性評価を手動/自動で実施すべき試験項目について検討を行い，明確化した。

In order to protect various systems from cyberattacks, it is essential to implement risk assessment and to adopt security measures appropriate for each type of attack. The need for accurate risk assessment has led to increasing demand for evaluation of the effects of cyberattacks on target systems and the difficulty levels of such attacks by actually conducting cyberattacks, in addition to the inspection of vulnerabilities. However, issues have been pointed out regarding the evaluation of cybersecurity from the standpoint of attackers, which is currently being carried out by only a limited number of experts with technical know-how referred to as ethical hackers.

To rectify this situation, the Toshiba Group is engaged in research and development aimed at realizing cyberattack emulation technologies that make it possible to automatically conduct offensive security tests. As part of this work, we have conducted studies on vulnerabilities of multifunctional peripherals (MFPs) equipped with multiple external interfaces as a motif. Based on the results of vulnerability assessments including offensive security tests carried out by an expert, we have clarified the test items for which assessments need to be performed either automatically or manually.

1. まえがき

重要な資産やサービスをサイバー攻撃の脅威から守るためには，サイバー攻撃に対するシステムへの影響や攻撃の難易度を明らかにしてセキュリティリスクを評価し，優先度を付けて対策することが重要である。

セキュリティリスクの代表例として，脆弱性がある。脆弱性の評価手法としては，共通脆弱性評価システム（CVSS）スコアが一般的であり，これを基に脆弱性への対応の優先度を決定することが多い。しかし実際には，悪用の事実や重要機能への影響などに基づいて，セキュリティ対策の優先度を決める必要がある。そのため，攻撃者視点で実際に攻撃を行う評価手法が，注目されている。

そこで，MFPサービス（MFPの機能を使ったサービスに加え，保守サービスなども含む）をモチーフとして，セキュリティリスクの評価を行った。MFPは，その名のとおり，様々な機能を備えているためインターフェースが多く，多様な視点でのセキュリティ評価が必要となる。このため，ほかの評価対象に比べて，応用展開しやすい。また，プリンター特有の通信プロトコルや制御言語を利用している点も制御システムと類似しており，制御システムへの応用展開も容易である。

MFPにおけるセキュリティ対策の取り組みとして，CC（Common Criteria）認証の取得がある。CC認証は，IT（情報技術）製品が備えるべきセキュリティ機能が，適正に開発されているかを評価する規格である。東芝テック（株）製のe-STUDIOシリーズは，複合機として最高レベルの基準HCD-PP（Hard Copy Device Protection Profile）に適合したCC認証を取得している。

一方MFPには，強固なセキュリティを必要とするCC認証に準拠した“ハイセキュリティモード”と，一般ユーザーが必要とするセキュリティ要件と使い勝手を両立させた“一般モード”があり，大多数のユーザーは一般モードを利用している。

ここでは，一般モードのユースケースを想定した脆弱性評価技術について述べる。また，このような脆弱性評価のノウハウを生かして，それらを自動的に行うことを目的としたサイ

バー攻撃エミュレーション技術の研究開発についても述べる。

2. 脆弱性評価技術

脆弱性評価は，目的別に脆弱性検査とサイバー攻撃耐性評価に分類できる。

2.1 脆弱性検査

脆弱性検査は，製品やシステムに内在する脆弱性を洗い出すことを目的としており，プラットフォーム脆弱性検査や，Webアプリケーション脆弱性検査，ファジング検査などがある（**図1**）。ここでは，試験プロセスにフォーカスを当てているため，ソースコードセキュリティ検査は除いた。

プラットフォーム脆弱性検査では，脆弱なバージョンのOS（基本ソフトウェア）・ソフトウェアを利用していないかや，セキュアなサービス設定をしているかなどを確認する。

Webアプリケーション脆弱性検査では，開発したWebアプリケーションに世の中で知られている脆弱性がないかを，確認する。OWASP JapanのWebアプリケーション脆弱性診断ガイドライン[1]を参照した手動チェックも含めている。

ファジング検査では，様々な細工を施したデータを送り，異常な動作を引き起こす未知の脆弱性を検出する。特に，事業分野特有の通信プロトコルを利用した検査が重要になる。

2.2 サイバー攻撃耐性評価

サイバー攻撃耐性評価は，製品やシステムに潜在するセキュリティリスクを把握することを目的としている。評価対象に内在する脆弱性を悪用したリスクだけでなく，同じ事業分野を対象とした脆弱性実証コードが悪用されるリスクや，セキュリティ設定の不備やセキュアではないプロトコルの利用に対するリスク，ネットワーク障害が引き起こされた際のリスクなどを，攻撃者視点で実際に攻撃を行って評価する。

サイバー攻撃耐性評価は，攻撃者視点で実際に攻撃してセキュリティリスクを評価するという点で，あらかじめ設定した攻撃を達成できるかどうかを評価するペネトレーションテストや，セキュリティオペレーションを評価するレッドチーミングテストの考え方に近い。しかし，それぞれ目的が異なるため，ここではサイバー攻撃耐性評価と呼ぶ。

サイバー攻撃耐性評価では，脆弱性検査で見付かった脆弱性が悪用された場合のセキュリティリスクや，脆弱性検査でカバーできていないセキュリティリスクを攻撃者視点で検証し，評価を行う。評価は，ペネトレーションテストと同様に，評価者の専門性や経験に依存する部分が大きいが，脆弱性検査結果に基づいてより多くの攻撃シナリオを検討するという点で異なる。

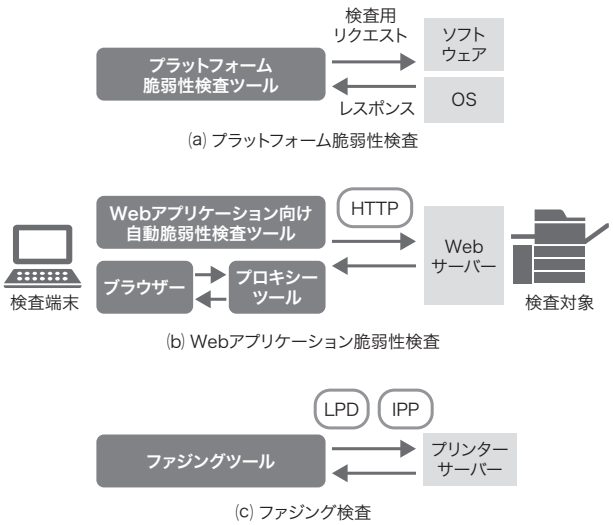


図1. 脆弱性検査の種類

脆弱性検査として，評価対象が提供しているサービスに対応したプラットフォーム脆弱性検査や，Webアプリケーション脆弱性検査，ファジング検査などがある。

Types of vulnerability tests

3. MFPサービスに対する脆弱性評価技術と自動化

3.1 MFPサービスに対する脆弱性検査

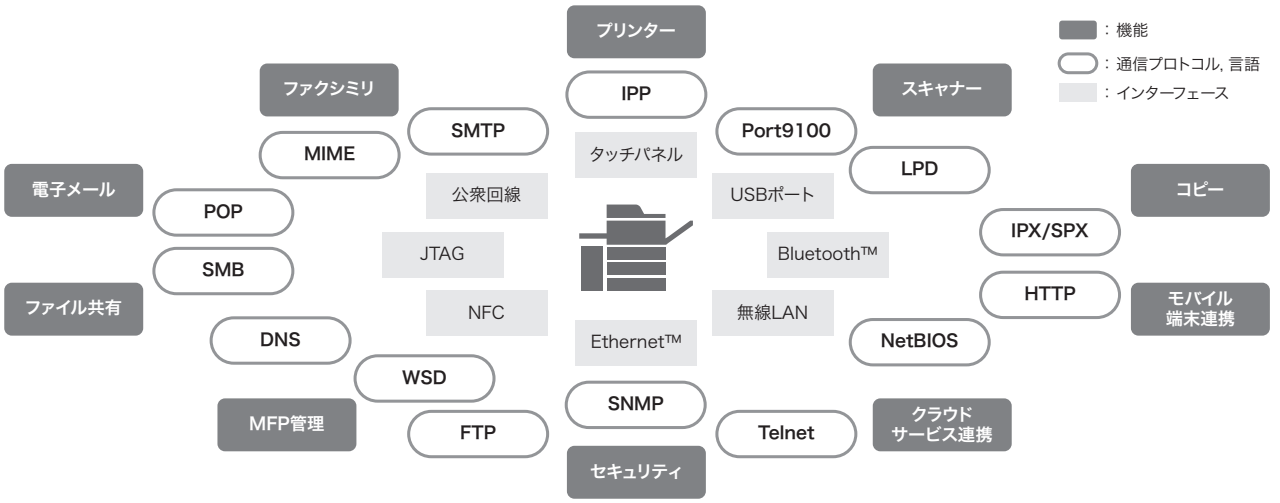
MFPは，コピー，プリンター，スキャナー以外にも様々な機能がある。また，プリンター機能では通信プロトコルのほかに，PJL（Printer Job Language）といったプリンター制御言語や，PostScript®・PCL™（Printer Command Language），PDF（Portable Document Format）などのページ記述言語で，印刷ジョブや印刷ドキュメントを制御している。そのため，MFPは様々なインターフェースや通信プロトコルを備えており（**図2**），これらを通して攻撃を受けるおそれがある。

サイバー攻撃からMFPを守るためには，MFPが備えているサービスやソフトウェアなどに適した脆弱性検査を行う必要がある。汎用的に適用可能なプラットフォーム脆弱性検査だけでなく，MFP管理に利用しているWebアプリケーションの脆弱性検査や，MFP分野で特有のプロトコルの処理部を開発している場合はファジング検査なども行う。

プリンター向けファジングツールとして，NCCグループが開発したFuzzowski[2]がある。NCCグループは，同ツールの適用やファームウェア解析を行い，6社のMFPに対して合計50件の新規脆弱性を明らかにした。そこで今回の脆弱性検査でも，このツールを利用してファジング検査を行った。

3.2 MFPに対するサイバー攻撃耐性評価

様々な評価を攻撃者視点で行うために，公開ドキュメントの評価，物理操作を伴う攻撃耐性評価，無線LAN経由の



IPX：Internetwork Packet Exchange
POP：Post Office Protocol
SNMP：Simple Network Management Protocol
USB：Universal Serial Bus
DNS：Domain Name System
SMB：Server Message Block
NetBIOS：Network Basic Input Output System
SMTP：Simple Mail Transfer Protocol
WSD：Web Services on Devices
JTAG：Joint Test Action Group
SPX：Sequenced Packet Exchange
MIME：Multipurpose Internet Mail Extensions
FTP：File Transfer Protocol
NFC：Near Field Communication

図2. セキュリティの視点から見たMFPの攻撃対象領域

MFPがサポートしている様々なインターフェースや通信プロトコルなどは，攻撃の糸口となり得る。

Security risk areas of MFP targeted by cyberattacks

攻撃耐性評価，MFP向けに開発された脆弱性実証コード・ツールの調査と耐性評価，及びネットワーク経由の攻撃耐性評価の5種類を実施した（**図3**）。

公開ドキュメントの評価は，インターネット又は顧客に公開しているMFPに関するドキュメントを調査し，サイバー攻撃に利用される情報が何かを攻撃者視点で評価した。

物理操作を伴う攻撃耐性評価は，タッチパネルや，キーボード・マウス，USB（Universal Serial Bus）メモリーなどを通しての悪用が可能かどうかを評価した。社内や委託先などの，MFPに直接接触可能な攻撃者を想定している。

無線LAN経由の攻撃耐性評価は，無線LAN通信を傍受し，共有キーを解析することで，無線LAN経由でMFPにアクセス可能かどうかを評価した。MFPへの攻撃については，後述するネットワーク経由の攻撃耐性評価と同様である。MFPを設置している敷地内に入ることができ，無線LANの届く範囲にいる攻撃者を想定している。

MFP向けに開発された脆弱性実証コード・ツールの調査と耐性評価は，プリンターに特化したセキュリティ評価ツールPRET[(3)]（Printer Exploitation Toolkit）を利用した。PRETは，評価対象のMFPに対して印刷ジョブや，プリンターのファイルシステム，メモリーなどが攻撃者に悪用されるかどうかを検証できる実績のあるツールである。このツールを開発したルール大学ボーフムは，20社のMFPに対してPRETを適用した結果，合計161件の新規脆弱性を明らかにした。そのほか，脆弱性実証コードのデータベースであるMetasploit™データベース及びExploitデータベースからMFPに関連する実証コードを調査した。例えば，2020年12月の調査では，Metasploit™データベースに30件程度，Exploitデータベースに150件程度のMFP関連脆弱性実証コードが見付かった。インターネット上に公開されたコード・ツールを悪用する攻撃者を想定している。

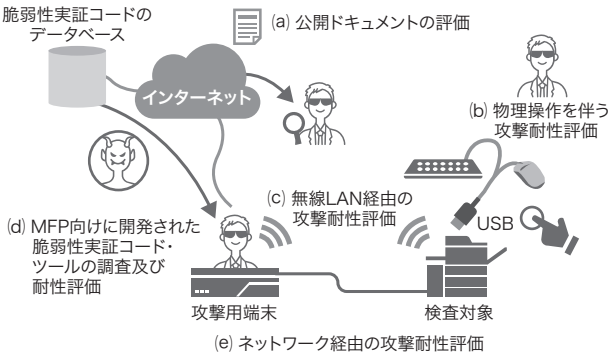


図3. MFPに対するサイバー攻撃耐性評価

MFPが備えているインターフェースやサービスに対応したサイバー攻撃耐性評価を，様々な攻撃者視点で行う必要がある。

Assessments of resistance of MFP against cyberattacks

ネットワーク経由の攻撃耐性評価は，脆弱性検査で見付かった脆弱性を悪用した攻撃のほか，マルウェアのアップロードや，構成情報の取得，ユーザー認証機能のバイパ

ス，通信暗号化されていないプロトコルを利用した場合などのセキュリティリスクを評価する。MFPと同一ネットワークからの攻撃者を想定している。

実際に開発中のMFPに対して，脆弱性検査だけでなくサイバー攻撃耐性評価を行った結果，開発プロセスの段階でMFPに潜在する脆弱性やセキュリティリスクを把握し，実際の攻撃者に悪用される前に，攻撃を受けた際に表示されるエラーページの表現や画面遷移の見直し，意図していないファイルやフォルダーに対するアクセス制限の確認などの対策を施すことができた。また，副次的効果として，セキュア実装の検証方法を改善するきっかけにもなった。

安全に利用できるMFPを提供するには，開発プロセスで脆弱性評価を行い，ユーザーの利便性とセキュリティリスクを把握して，提供すべき機能と提供すべきでない機能を見分けることが重要である。その際に，攻撃者視点でセキュリティリスクを検討・実証することが，有用である。

3.3　サイバー攻撃耐性評価の自動化

脆弱性検査は既にツール化されており，開発プロセスに組み込みやすい。一方，サイバー攻撃耐性評価は属人的な部分が多く，開発プロセスに組み込みにくい。

MFPに対するサイバー攻撃耐性評価の経験に基づいて，手動／自動で実施すべき区分を検討した。その結果，公開ドキュメントの評価，物理操作を伴う攻撃耐性評価，無線LAN経由の攻撃耐性評価の３種類については自動化が難しく，MFP向けに開発された脆弱性実証コード・ツールの調査と耐性評価，ネットワーク経由の攻撃耐性評価の２種類については自動化が可能なことが分かった。ただし，評価対象に合わせて既存の脆弱性実証コードを改変したり，攻撃耐性評価を行うコード・ツールを評価者が実装したりといったことが必要であり，その部分の自動化は難しい。

東芝グループは，サイバー攻撃耐性評価の一部を自動化する技術（サイバー攻撃エミュレーション技術）の研究開発を進めている。そして，米国Peraton Labs社と共同で，サイバー攻撃エミュレーションツール“Automated Attack Path Planning and Validation”[(4)]を開発した。

開発したサイバー攻撃エミュレーションツールは，推論エンジンを用いて事前に行った脆弱性検査結果から，一連の攻撃の流れを示す攻撃シナリオを生成する。そして，攻撃実行エンジンを用いて，生成した攻撃シナリオに基づいたサイバー攻撃耐性評価を行う。推論エンジンが用いる攻撃パターンデータベースは，脆弱性と攻撃手順とを対応付けて登録でき，実機での攻撃評価が可能な攻撃シナリオを生成できることが特長である。

したがって，MFPに対するサイバー攻撃耐性評価に今回開発したサイバー攻撃エミュレーションツールを適用することで，IP（Internet Protocol）アドレスや認証情報などを設定すれば脆弱性実証コード・ツールを用いた攻撃耐性評価を自動化できる見込みが得られた。

4.　あとがき

MFPをモチーフとして，サイバー攻撃から守るための脆弱性評価技術について述べた。また，脆弱性評価を開発プロセスに組み込むことを目的とした，サイバー攻撃エミュレーション技術の研究開発についても述べた。

今後は，脆弱性評価技術を開発プロセスに取り入れるとともに，これらの知見をサイバー攻撃エミュレーション技術に組み込み，MFPサービスだけでなく産業制御システム全般のセキュリティ向上につながる仕組みを整えていく。

文　献

(1) OWASP Japan. "OWASP Japan Local Chapter Meetup | OWASP Foundation". OWASP Foundation. <https://owasp.org/www-chapter-japan/>, (参照 2022-01-07).
(2) GitHub, Inc. "GitHub – nccgroup/fuzzowski: the Network Protocol Fuzzer that we will want to use.". GitHub. <https://github.com/nccgroup/fuzzowski>, (accessed 2021-12-17).
(3) GitHub, Inc. "GitHub – RUB-NDS/PRET: Printer Exploitation Toolkit – The tool that made dumpster diving obsolete.". GitHub. <https://github.com/RUB-NDS/PRET>, (accessed 2021-12-17).
(4) GitHub, Inc. "A2P2V · GitHub". GitHub. <https://github.com/pentest-a2p2v/>, (accessed 2022-01-31).

青木　　慧　AOKI Satoshi
研究開発センター サイバーセキュリティ技術センター
セキュリティ基盤研究部
電子情報通信学会会員
Security Research Dept.

春木　洋美　HARUKI Hiroyoshi
研究開発センター サイバーセキュリティ技術センター
セキュリティ運用推進部
情報処理学会会員
Managed Security Dept.

佐藤　俊至　SATO Toshiyuki
東芝テック（株）ワークプレイス・ソリューション事業本部
ソリューション技術部
Toshiba Tec Corp.