資料２

直近のインシデントについて

総 務 省

令和７年１月31日

総務省自治行政局

デジタル基盤推進室

テレワークシステム（VDI）への不正アクセスについて

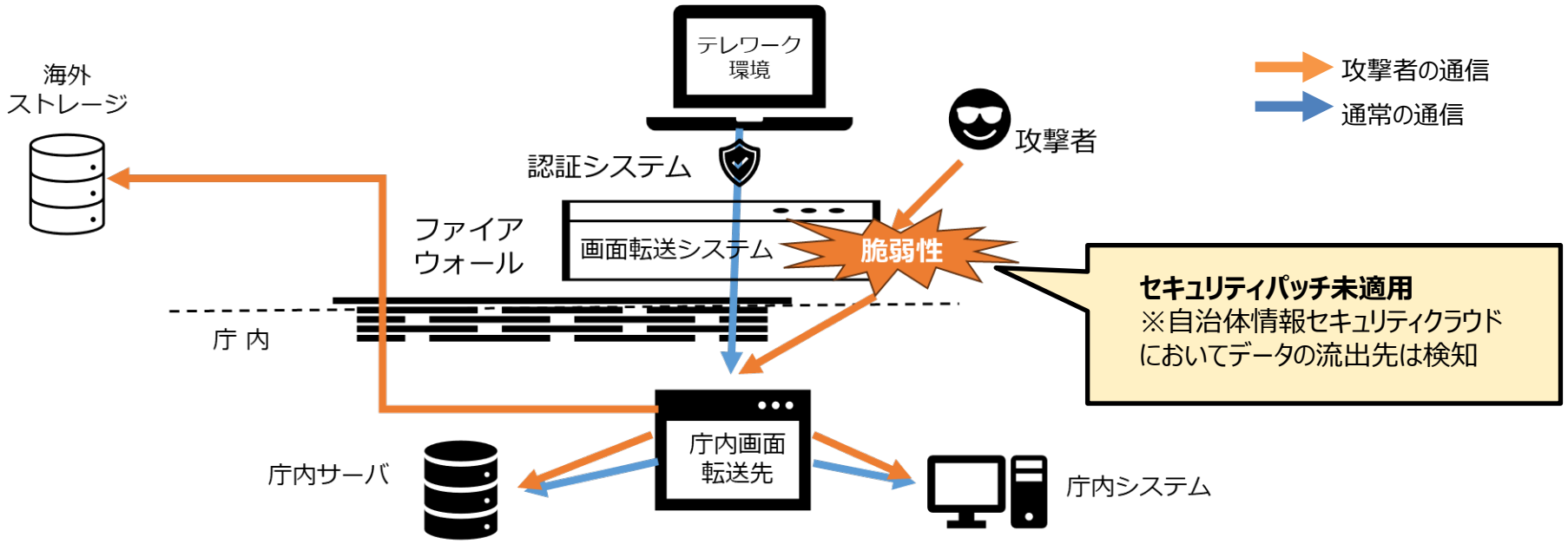
事案の概要

■ 団体Aにおいて、テレワークシステム（仮想デスクトップ（VDI）方式で庁内ネットワークに接続し、業務を行うもの）が脆弱性を突く攻撃を受け、攻撃者が職員3名のアカウントになりすましてVDIにログインする不正アクセスが行われた。

■ テレワークシステムのログに、不正アクセス時に外部のオンラインストレージ等にアクセスしてデータのアップロードが行われた形跡があり、情報漏洩が発覚した。

原 因

■ 直接の原因は、テレワークシステムの認証機能を担うネットワーク機器にセキュリティパッチが適用されておらず、その脆弱性を突かれて認証が突破されたことによるもの。



必要な対策

- 再発防止、被害拡大防止、相談先の確保の３つの観点から対策を示す。
- 各用語については次ページ以降において解説。

	課 題	対策の方向性	対 策
再発防止	• リモートワーク用のVDIのセキュリティパッチが適用されていなかった。 脆弱性により、認証を回避され既に作成済みのセッションを攻撃者に悪用され侵入を許した。 • ベンダとの契約においてセキュリティパッチの適用回数に上限が設定されていた。	• 効果的なパッチ選定とパッチ適用	**【 組織的対策 】** ● **ベンダとの契約の中に、パッチ適用のみならず、影響度と緊急度の高い脆弱性の把握や実際に適用するかの判断など、適用に至るまでのプロセスまで含める（ソフトウェア以外のネットワーク機器等についても脆弱性を確認し、対応が必要なことに留意する）。** ● **脆弱性の影響度合の確認のため、ベンダーにソフトウェアの構成部品のリスト化を依頼（SBOMの活用も考慮）**
被害拡大防止	• 外部ストレージへの情報の送信を止めることができなかった。	• 第3者による保有情報へのアクセスの防止	**【 技術的対策 】** ■ **アクセス時に認証が可能なシステムに情報を格納し、認証を実施するようにする。** ■ **アクセス権限を付与する範囲の最小化** ■ **EDR、NDR※等による不正なアクセス動作の検知**
		• 情報の意図しない外部漏えいの防止	**【 技術的対策 】** ■ **DLP※ツールの導入** **（資産の重要度のラベリング）**
相談先の確保	• インシデント対応（分析、封じ込め、根絶等）に協力してくれる相談先の確保に時間を要した。	• インシデント時の対応を依頼可能な相談先の確保	**【 組織的対策 】** ● **インシデント対応依頼が可能なベンダのリスト化** ● **インシデント対応依頼なベンダとの定期的な情報共有** **（システム構成の共有、パートナーシップの強化）** ● **開発ベンダとインシデント発生時の役割について明確化**

※ EDR、NDR、DLPについての説明はP8をご参照。

各対策の詳細（再発防止）①

対策：再発防止	地方公共団体における情報セキュリティポリシーに関するガイドライン（以下「ガイドライン」という。）の方向性
● **ベンダとの契約の中に、パッチ適用のみならず、影響度と緊急度の高い脆弱性の把握や実際に適用するかの判断など、適用に至るまでのプロセスまで含める（ソフトウェア以外のネットワーク機器等についても脆弱性を確認し、対応が必要なことに留意する）。**	• 重要度の高い脆弱性の把握について、以下の統一基準群における規定を参考にし、ガイドラインに新たに規定してはいかがか。 • 地方公共団体のリソース不足を考慮し、**脆弱性の把握やパッチ適用の判断の実施について、ベンダとの契約に入れることについてもガイドラインに新たに規定**してはいかがか。 **政府機関等の対策基準策定のためのガイドライン（令和５年度版）** **5.2.3 情報システムの運用・保守** **（解説）** **● 基本対策事項5.2.3(1)-6「脆弱性の存在が明らかになった場合」について** 機関等が運用する情報システムに関連する脆弱性が存在することが発覚した場合、セキュリティパッチの適用等の情報セキュリティ対策が必要となる。そのためには、**公開された脆弱性についての影響度と緊急度を判断する必要がある。緊急度を判断するためには、公開された脆弱性の深刻度を示すCVSS（Common Vulnerability Scoring System）の値や当該脆弱性を悪用した攻撃の段階（例えば、脆弱性を用いた攻撃手法が出回ってる、既に脆弱性を用いた攻撃が確認されている等）などを考慮して検討するとよい。**

補足

◆**CVSS（Common Vulnerability Scoring System）**

公開された脆弱性の深刻度を示す指標。深刻度は0(低)～10.0(高)の数値で表される（7.0以上が重要、9.0以上が緊急）。CVSSの値はJPCERT/CC及び独立行政法人情報処理推進機構（IPA）のWebサイト「脆弱性対策情報データベース」で確認することができる。

＜参考：JPCERT/CC及び独立行政法人情報処理推進機構 「脆弱性対策情報データベース」＞
https://jvndb.jvn.jp/
＜参考： 独立行政法人情報処理推進機構（IPA）「共通脆弱性評価システムCVSS v3概説」＞
https://www.ipa.go.jp/security/vuln/scap/cvssv3.html

ガイドライン改定案①

➢ 情報システムの運用に係る解説に、注書きで追記する形にしてはいかがか。

改定案：対策基準（解説）

７．運用
7.1.情報システムの監視
(１)情報システムの運用・保守時の対策

①「監視を含むセキュリティ機能」について
（略）
②「見直し」について
（略）

（注）地方公共団体が運用する情報システムに関連する脆弱性が存在することが発覚した場合、セキュリティパッチの適用等の情報セキュリティ対策が必要となる。公開された脆弱性についての影響度と緊急度を判断する必要がある。緊急度を判断するためには、公開された脆弱性の深刻度を示すCVSS（Common Vulnerability Scoring System）の値や当該脆弱性を悪用した攻撃の段階（例えば、脆弱性を用いた攻撃手法が出回ってる、既に脆弱性を用いた攻撃が確認されている等）などを考慮して検討するとよい。このとき、ソフトウェア以外のネットワーク機器等についても脆弱性を把握し適切な対策を行う必要があることに留意する。可能な限りすべてのセキュリティパッチを適用することが望ましいが、インターネットとの境界にある機器におけるセキュリティパッチの適用は特に重要である。また、ベンダとの契約の中に、パッチ適用のみならず、影響度と緊急度の高い脆弱性の把握や実際に適用するかの判断など、適用に至るまでのプロセスまで含めることで、自団体に十分なリソースがない場合でも、効果的なパッチ適用を行うことが可能になる。

なお、CVSSの値は以下のウェブサイトで確認できる。

参考：JPCERT/CC及び独立行政法人情報処理推進機構「脆弱性対策情報データベース」
https://jvndb.jvn.jp/
参考：独立行政法人情報処理推進機構「共通脆弱性評価システムCVSS v3概説」
https://www.ipa.go.jp/security/vuln/scap/cvssv3.html

脆弱性が顕在化しているにも関わらず、やむを得ず対応できない場合は、一時的な回避方法として、当該ソフトウェア等に関係するベンダが公開した緩和策をとることが考えられる。

各対策の詳細（再発防止）②

対策：再発防止	ガイドラインの方向性
● **脆弱性の影響度合の確認のため、ベンダーにソフトウェアの構成部品のリスト化を依頼（SBOMの活用も考慮）**	• 統一基準群改定を踏まえ、ガイドラインにはSBOMの活用を規定することとしている（第15回検討会で提示）。 **ガイドライン改定案** **6.3. システム開発、導入、保守等** 【解説】 （２） 機器等及び情報システムの調達 （中略） SBOMとは、ソフトウェアコンポーネントに関する情報を含んだ機械処理可能な一覧リストのことで、オープンソースソフトウェアに関する情報だけではなく、プロプライエタリソフトウェア（ソフトウェア配布者がその知的財産を保持しており、改変や複製が制限されているソフトウェア）に関する情報も含めることができる。ソフトウェアに関する選定基準の一つとして、SBOMの情報を地方公共団体が確認できることに関する基準を加えることで、ソフトウェアの透明性の確認を行うことができる。さらに、**脆弱性に関する対策の効率化の観点からSBOMを活用することも考えられる**。SBOMの項目は多様であり、SBOMの対応範囲に応じてコストと効果が大きく異なるため、分野やシステム利用環境のリスクの違いに応じて妥当な対応範囲を目指すことが効果的である。従って、選定基準においては、SBOMの提供有無の二者択一ではなく、SBOMの対象とするソフトウェアの範囲や脆弱性管理の範囲等について、対象ソフトウェアのリスクを踏まえ、調達先への過度な要求とならない範囲で明示するとよい。例えば、利用時のリスクが低いソフトウェアについては、最小限のSBOM対応範囲に留めることなどにより、コストを抑えることも考えられる。

補足

◆ **SBOM（Software Bill of Materials）**

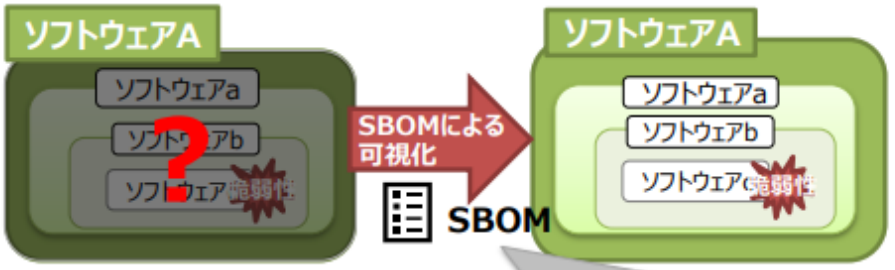
ソフトウェアコンポーネントに関する情報を含んだ機械処理可能な一覧リスト。近年、ソフトウェアの脆弱性管理に関し、ソフトウェアの開発組織と利用組織双方の課題を解決する一手法として、SBOMを用いた管理手法が注目されている。

＜参考： ソフトウェア管理に向けたSBOM（Software Bill of Materials）の導入に関する手引 ver 2.0（令和６年８月29日経　済産業省商務情報政策局サイバーセキュリティ課）＞
https://www.meti.go.jp/press/2024/08/20240829001/20240829001.html

ソフトウェア・セキュリティ確保手段としてのSBOM

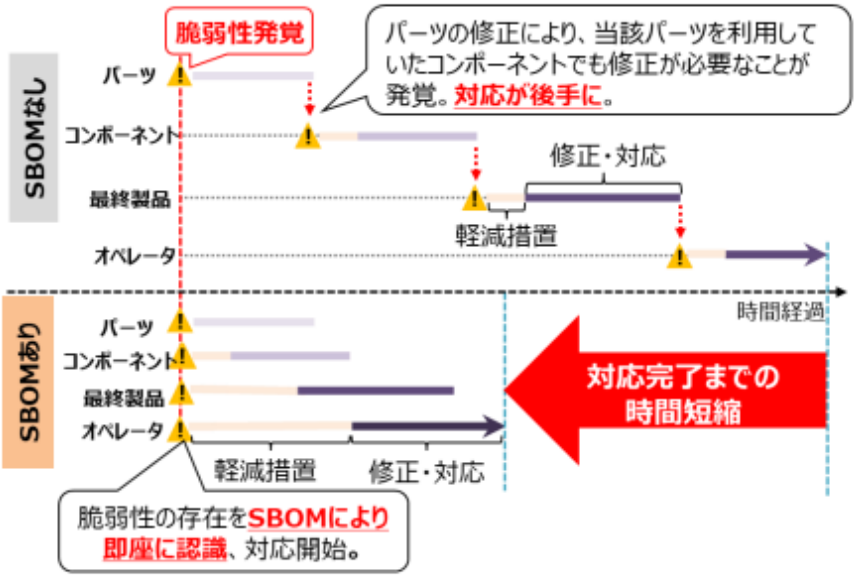
- SBOM （Software Bill of Materials）とは、**ソフトウェアの部品構成表**のこと。ソフトウェアを構成する**各部品（コンポーネント）を誰が作り、何が含まれ、どのような構成となっているか**等を示す。
- SBOMによりソフトウェアの構成情報を詳細に把握することができるため、脆弱性情報の即時の特定が可能であり、**脆弱性対応などへの活用が期待**できる一方、その作成効果やコストなどの課題が存在するため、実証による検証を実施。
- 2023年7月、**「ソフトウェア管理に向けたSBOMの導入手引ver1.0」を公表**。SBOMに関する基本的な情報や導入に向けた実施事項のポイントを示す。

<SBOMイメージ>



サプライヤ名	コンポーネント名	バージョン	製品URLなど	…
A会社	ソフトウェアA	Ver1.0	……	…
A会社	|…ソフトウェアa	Ver2.1	……	…
B会社	|…ソフトウェアb	Ver5.3	……	…
C会社	|…ソフトウェアc	Ver1.2	……	…

SBOMの導入効果：脆弱性発覚から復旧までの時間を短縮



（参照元：「『ソフトウェア管理に向けたSBOM（Software Bill of Materials）の導入に関する手引ver2.0』の概要について」（令和６年８月29日経済産業省商務情報政策局サイバーセキュリティ課）

各対策の詳細（被害拡大防止）

対策：被害拡大防止	ガイドラインにおける規定
■ **アクセス時に認証が可能なシステムに情報を格納し、認証を実施するようにする。** ■ **アクセス権限を付与する範囲の最小化** ■ **EDR、NDR等による不正なアクセス動作の検知**	• 所管するネットワーク又は情報システムごとに、アクセスする権限のない者がアクセスできないよう制限することについて、「6.2 アクセス制御 (1)アクセス制御等」に規定。 • 未知の不正プログラムへの対策（エンドポイント対策）は「3. 情報システム全体の強靭性の向上」で規定（β、β'モデルでは必須、α'モデルでは推奨）しているが、**どのようなサービスを選定すべきか評価基準について規定**する。 • 情報窃取等の不正な動作を監視し、検知・防止する仕組みについて「7.1 情報システムの監視(2)情報システムの監視機能」に規定。 **現行ガイドライン** **6.2.アクセス制御** 【例文】 （１）アクセス制御等 ①アクセス制御 統括情報セキュリティ責任者又は情報システム管理者は、**所管するネットワーク又は情報システムごとにアクセスする権限のない職員等がアクセスできないように必要最小限の範囲で適切に設定する等、システム上制限しなければならない**。 **7.1.情報システムの監視** 【解説】 （２）情報システムの監視機能 ①「監視機能を実装」について （略）**職員等による情報窃取等の不正な動作を監視し、これらの不正な動作を検知・防止する内部脅威対策機能を備えたDLP の仕組みの導入を検討してもよい**。

補足

◆ **EDR（Endpoint Detection and Response ）、NDR (Network Detection and Response)**
不正プログラムの挙動を検知する方式等によって既知及び未知の不正プログラムの検知並びにその実行を防止するもの。

◆ **DLP （Data Loss Prevention）**
情報窃取等の不正な動作を監視し、これらの不正な動作を検知・防止する内部脅威対策機能を備えているもの。

各対策の詳細（相談先の確保）・ガイドライン改定案②

✓ 今回の事案のようにな**不正アクセスがあった場合、異常な挙動の端末を監視・検出・特定することが一層重要となる**ことから、α'モデルやβ・β'、モデル、マイナンバー利用事務系に係る画面転送方式の対策の１つとして提示している**「未知の不正プログラム対策」につき、以下のとおり厳密に規定**する。

現行

＜未知の不正プログラム対策＞
　従来のパターンマッチング型の検知に加えて、セキュリティ専門家によるマネージドサービスの運用により、エンドポイントのアクティビティを監視し、未知及び既知のマルウェア等による悪意ある活動を示す異常な挙動の端末を監視・検出・特定する。また、異常な挙動を検出した際にプロセスを停止し、ネットワークから論理的な隔離を実施する。さらにインシデント発生要因の詳細な調査を実施する。

改定案

＜未知の不正プログラム対策＞
　従来のパターンマッチング型の検知に加えて、セキュリティ専門家によるマネージドサービスの運用により、エンドポイントのアクティビティを監視し、**外部からの侵入や、未知及び既知のマルウェア等による悪意ある活動（データの持ち出しや外部との通信等）**を示す異常な挙動の端末を監視・検出・特定する。また、異常な挙動を検出した際にプロセスを停止し、ネットワークから論理的な隔離を実施する。さらにインシデント発生要因の詳細な調査を実施する。
サービスを選定する際には、以下の観点で評価することが考えられる。
・当該サービスにより、その団体の情報が国外に持ち出される可能性があるか。
・マネージドサービスが国内で提供されているか。
・セキュリティ専門家の経歴
・監視・検出・特定を行う際に使用する機器等のセキュリティ対策

各対策の詳細（相談先の確保）・ガイドライン改定案③

対策：相談先の確保	ガイドドラインの規定・方向性
● インシデント対応依頼が可能なベンダのリスト化 ● インシデント対応依頼ベンダとの定期的な情報共有（システム構成の共有、パートナーシップの強化） ● 開発ベンダとインシデント発生時の役割について明確化	• 「第3編　第2章 1.組織体制 (9)CSIRT の設置・役割」に有事の際においても専門家との連携ができるようにしておくことが望ましいことが規定されている。 • 専門家との連携が困難であり、対応が遅れてしまう場合が生じうることを考慮し、**ベンダとの連携についてもガイドラインに新たに規定**することとしてはいかがか。

現行：対策基準（解説）

Ⅰ．組織体制
（９）CSIRT の設置・役割

（注12）CSIRT の設置においては、役割を明確にする必要があるため、以下を参考に構築や役割の明確化を実施することが望ましい。
（略）
また、地方公共団体情報システム機構（自治体CEPTOAR 事務局）等の関係機関や他の地方公共団体における同様の窓口機能、委託事業者、有識者及び専門家等と連携して体制を強化するとともに、有事の際においても専門家との連携ができるようにしておくことが望ましい。

改定案：対策基準（解説）

Ⅰ．組織体制
（９）CSIRT の設置・役割

（注12）CSIRT の設置においては、役割を明確にする必要があるため、以下を参考に構築や役割の明確化を実施することが望ましい。
（中略）
また、地方公共団体情報システム機構（自治体CEPTOAR 事務局）等の関係機関や他の地方公共団体における同様の窓口機能、委託事業者、有識者及び専門家等と連携して体制を強化するとともに、**有事の際においても専門家との連携ができるようにしておくことが望ましい。専門家との連携が難しい場合においては、インシデント対応**（分析、封じ込め・根絶等）**依頼が可能なベンダのリスト化、当該ベンダとの定期的な情報共有などにより、迅速な対応が可能になる。このような相談先の候補として、経済産業省が定める「情報セキュリティサービス基準」及び当該基準を満たすと認められた企業を掲載した「情報セキュリティサービス基準適合サービスリスト」のうち、デジタルフォレンジックサービス部分も参考になる。また、このような相談先とあらかじめNDA（秘密保持契約）を結んでおくことで、インシデントが発生した際に迅速な対応が可能になる。**
参考：独立行政法人情報処理推進機構「情報セキュリティサービス基準適合サービスリスト」
https://www.ipa.go.jp/security/service_list.html

補足

◆「**情報セキュリティサービス基準適合サービスリスト**」
特定非営利活動法人日本セキュリティ監査協会（JASA）が、経済産業省が定める「情報セキュリティサービス基準」に適合するか否かの審査・判定を行った事業者が掲載。「デジタルフォレンジックサービス」のリストの企業の中には、緊急の初動対応やインシデントの原因特定・封じ込め等を実施する旨が記載されているものもある。