～成果発表課題～

三菱電機事案

内堀紘徳

目次

目次

事象

「三菱電機事案」

- 2020年1月20日，三菱電機は自社ネットワークが
  不正アクセスを受け，個人情報が外部へ流出した可能性が
  あると発表.
- 流出した情報には，個人情報や企業機密の他に
  防衛関連情報が含まれており，社会的な注目を浴びた事案
- 従来の監視や検知をすり抜ける高度かつ巧妙な手法で，
  ログの削除，送信元IPアドレス詐称などにより調査が
  難航した.

影響（情報流出の観点）

- 流出した可能性のある情報

＜個人情報＞

- 採用応募者（1,987人）
- 従業員（4,566人）
- グループ関係退職者（1,569人）

＜企業機密情報＞

- 執行役員会議資料
- 研究所内で共有された週報
- 数十社との共同開発，商談，製品受注等の取引関連情報
- 防衛省，JAXA等10を超える政府，官公庁とのやりとりの情報

＜防衛省の機微情報＞

- 装備品に関する研究試作入札関連情報で防衛省の定める注意情報
- 装備品の研究試作に関連する資料
- 研究試作に関連する落札方式の評価規準，研究施策の性能要求事項

三菱電機「不正アクセスによる個人情報と企業機密の流出可能性について」，piyolog より

影響（被害範囲）

- 社内ネットワークのPC24.5万台を調査

感染の疑いが確認された端末	132台
重要な情報にアクセス可能な端末	国内9台，中国拠点確認中

三菱電機「不正アクセスによる個人情報と企業機密の流出可能性について（第3報）」より

- ログの消去や送信元アドレスの詐称により，攻撃者や被害範囲の特定は難航.

影響（社会的側面）

- 「国家安全保障上の脅威情報がサイバー攻撃で漏洩したことを、当局が公に認めた初のケース」（内閣官房関係者）

流出ファイル59件が安全保障に影響か　三菱電機へのサイバー攻撃

成沢解語　2021年12月24日 21時21分

シェア　ツイート　ブックマーク　メール　印刷

list　1

三菱電機のロゴマーク

三菱電機 が大規模な サイバー攻撃 を受けた問題で、 防衛省 は24日、外部に流出した可能性がある防衛関連のデータファイルのうち、安全保障に影響を及ぼすおそれのあるファイルが59件あったと発表した。すでに対策を講じ、22日付で同社を口頭で注意した。

中国の影、たどり着いた雑居ビル　三菱電機サイバー攻撃 →

朝日新聞 より

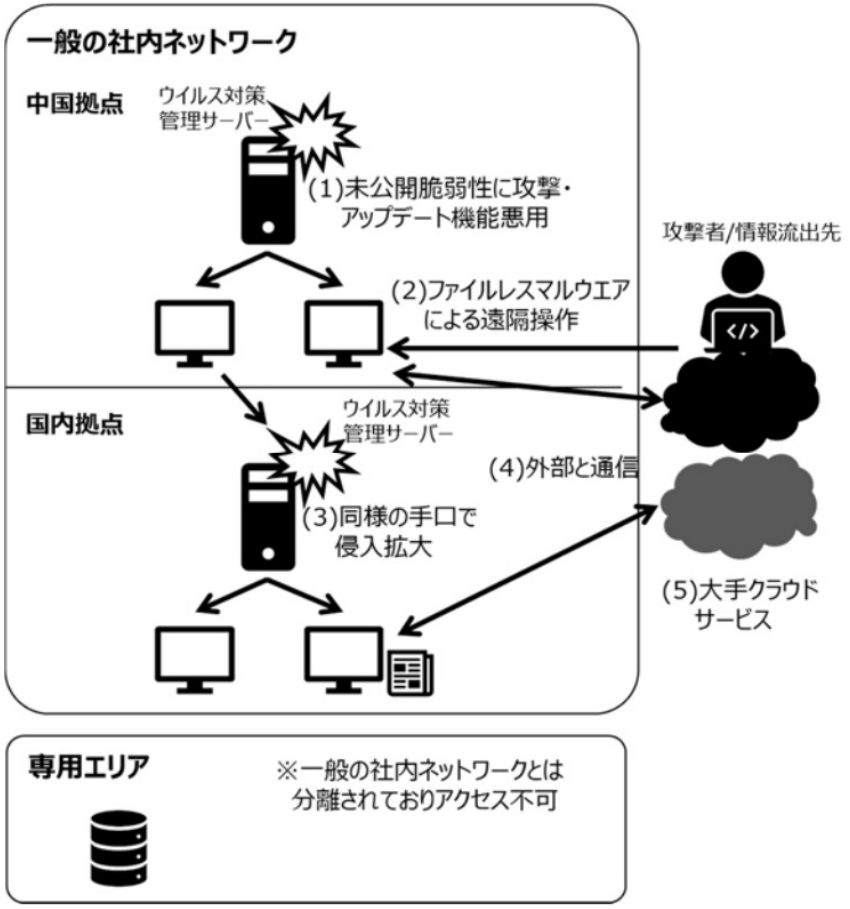
タイムライン

2019/06/28	**ウイルス対策ソフトにより，国内拠点の端末で不審な挙動を検知**
2019/07/08	社内ネットワークに不正アクセスされている事実を把握.
2019/07/10	社内端末24.5万台の調査により国内外の複数拠点侵害の可能性が高いと判断.
2019/07/17	**不正な通信先をすべて特定して遮断．封じ込め完了と判断.**
2019/08/01	保全が完了した端末から，フォレンジック調査など，詳細な解析を開始.
2019/08/29	未公開脆弱性情報，マルウェア情報，不正通信先アドレス情報をJPCERT/CCに報告
2019/08/31	流出可能性ファイルの仕分けを実施
2019/09-10	Trend Micro， JPCERT/CCがウイルスバスター製品の脆弱性を公表.
2020/01/20	**三菱電機が不正にアクセスによる情報流出を発表（第1報）.** 朝日新聞報道

三菱電機「不正アクセスによる個人情報と企業機密の流出可能性について（第3報）」，piyolog より

目次

攻撃手口と侵入経路

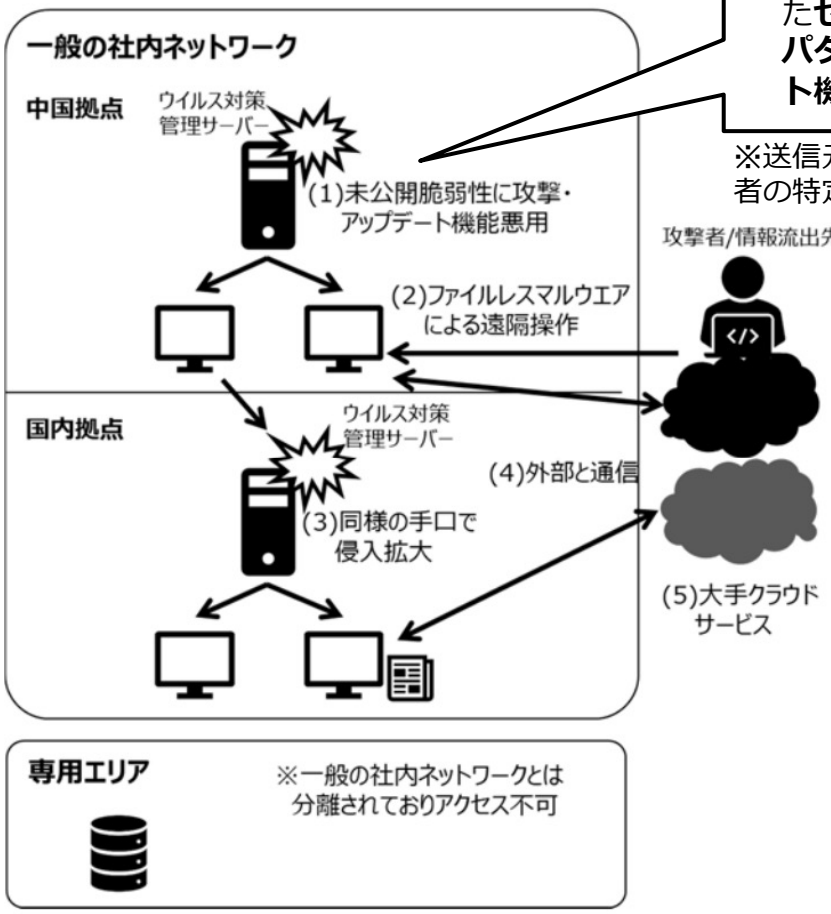


三菱電機「不正アクセスによる個人情報と企業機密の流出可能性について（第3報）」より

攻撃手口と侵入経路

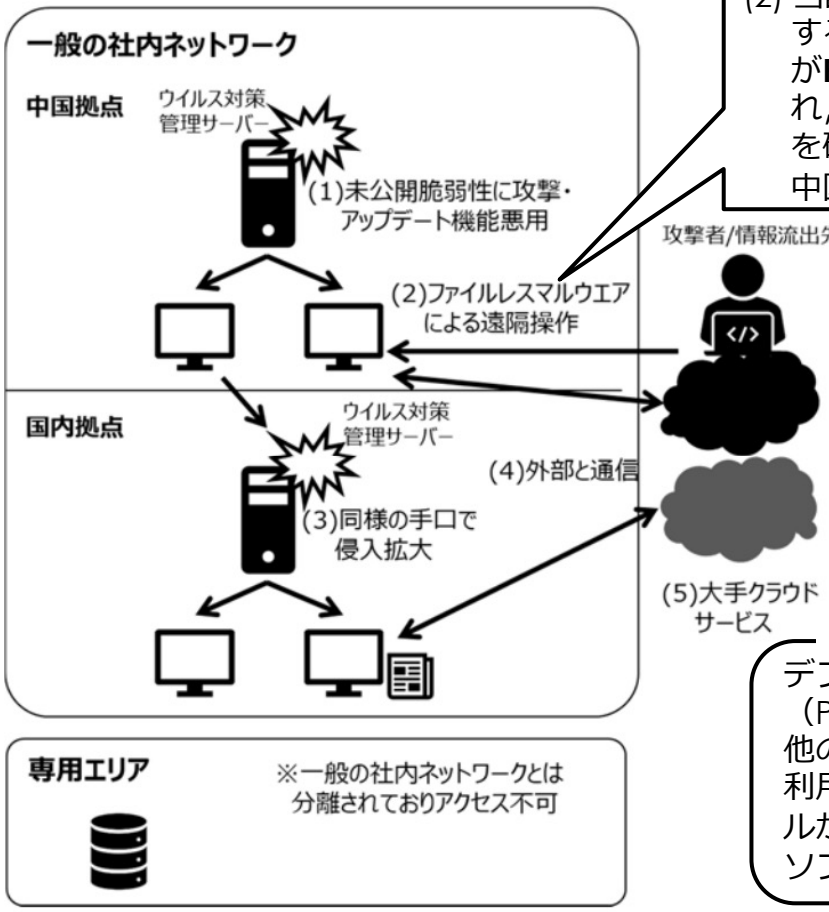
(1) 中国拠点のウイルス対策サーバが未公開脆弱性を突いた**ゼロデイ攻撃**受ける．**パターンファイルアップデート機能**が悪用され侵入が拡大．

※送信元アドレスの詐称により攻撃者の特定が難航



三菱電機「不正アクセスによる個人情報と企業機密の流出可能性について（第3報）」より

攻撃手口と侵入経路



(2) 当該端末のメモリー内で活動する**ファイルレスマルウェア**が**PowerShell**を用いて実行され，外部からの**遠隔操作攻撃**を確立．
中国内他拠点に感染拡大．

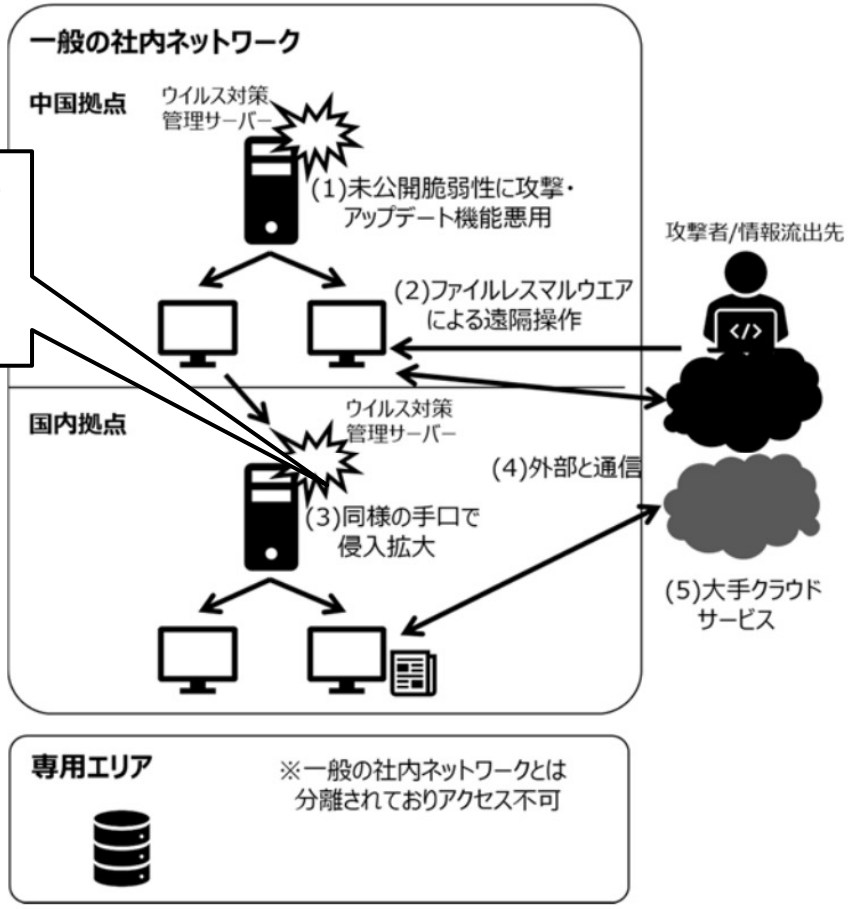
ファイルレスマルウェア

デフォルトのWindowsツール（PowerShell）などを利用して，他のマシンに展開する．メモリが利用され，ディスク上にはファイルが存在しないためウイルス対策ソフトなどでの検出が困難．

三菱電機「不正アクセスによる個人情報と企業機密の流出可能性について（第3報）」より

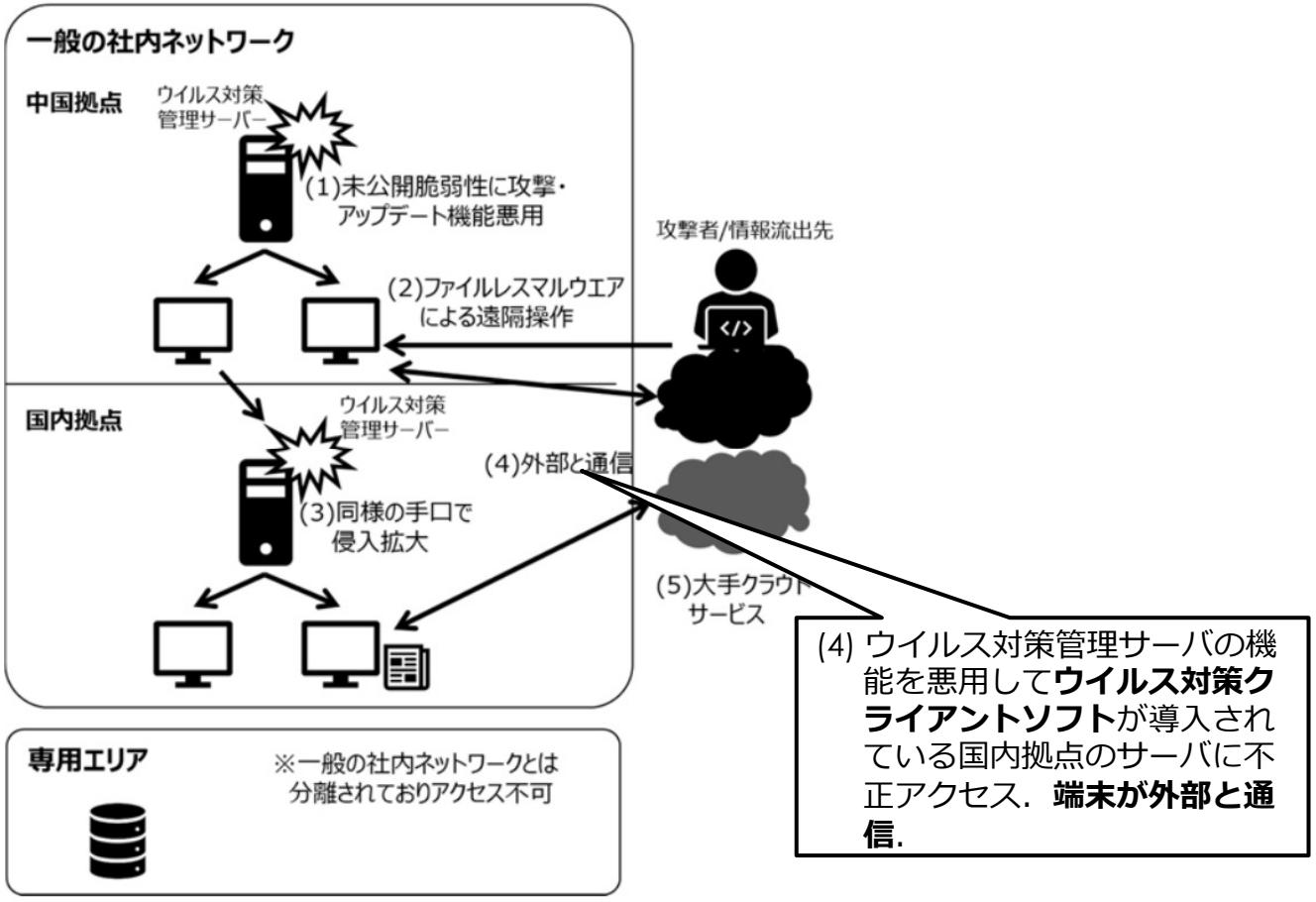
攻撃手口と侵入経路

(3) 中国拠点のウイルス対策管理サーバを介して，日本国内のウイルス対策管理サーバを**同様の手口**で攻撃．国内複数拠点に侵入拡大．



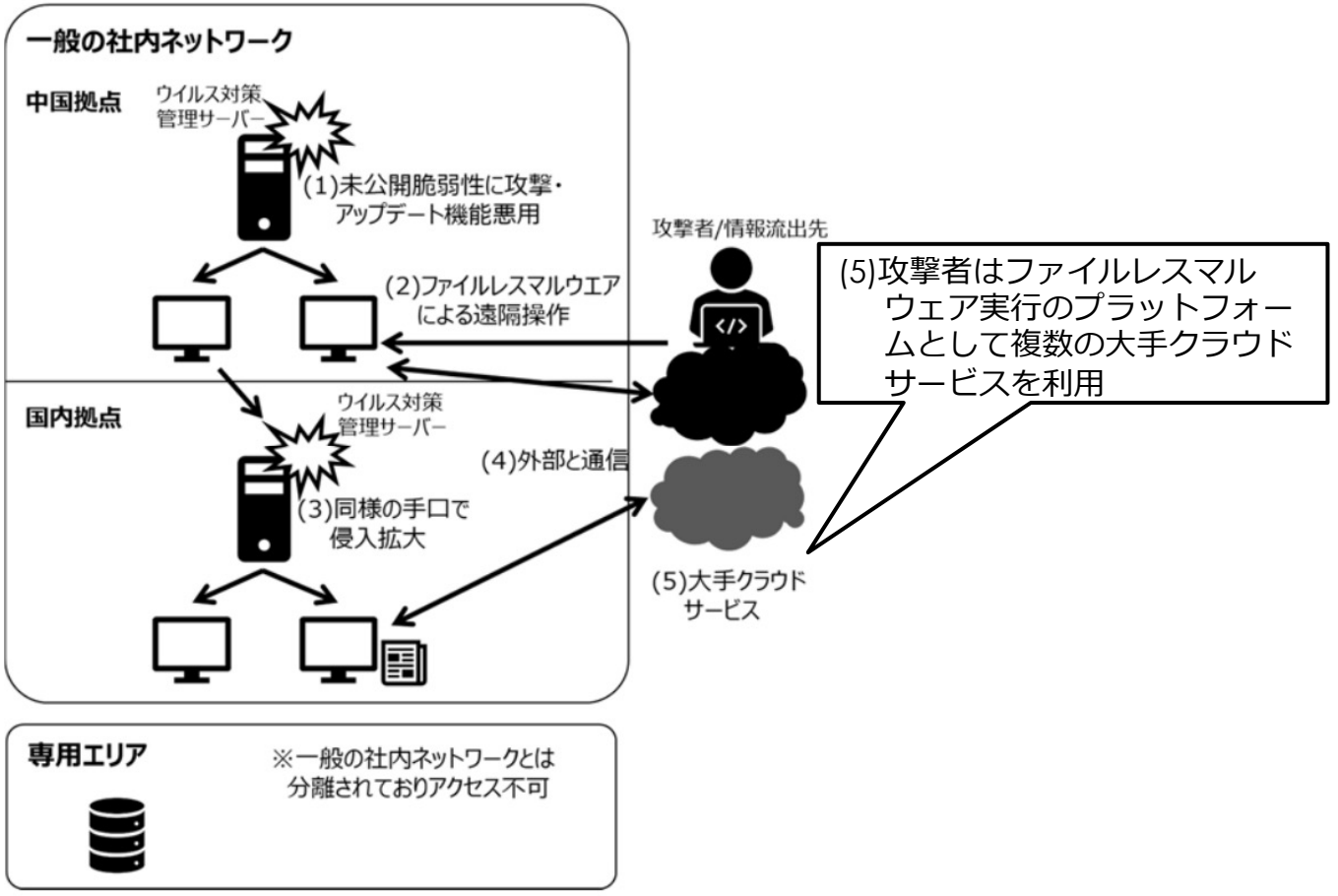
三菱電機「不正アクセスによる個人情報と企業機密の流出可能性について（第3報）」より

攻撃手口と侵入経路



三菱電機「不正アクセスによる個人情報と企業機密の流出可能性について（第3報）」より

攻撃手口と侵入経路



三菱電機「不正アクセスによる個人情報と企業機密の流出可能性について（第3報）」より

拠点間の感染拡大

- この攻撃では，拠点間の感染拡大（横展開）にVPNが悪用されている．（朝日新聞の調査）
  ⇨ 一旦内部に侵入されると脆弱性が残っている場合は感染が拡大しうる（内部のセキュリティは見落とされがち）
- 中国拠点のVPN装置（米パルス・セキュア社製）の欠陥が利用されたとみられる．
- 攻撃は欠陥公表の2ヶ月前であった．
- 高度な技術力を持った中国系サイバースパイ集団による攻撃と考えられる．

侵入の防御が困難であった面もある

目次

被害は防げたか

- 防御が困難であったと考えられる点
  - ネットワークへの侵入・感染拡大
    ⇨ 未公開脆弱性を利用した**ゼロデイ攻撃**であった.

- 対策可能であったと考えられる点
  - 防衛関連情報の流出
    ⇨ 防衛省が「注意情報」として複製を禁じていたが，三菱電機が**無断で電子化（PDF化）**して保存していた.
    （三菱電機は防衛省に対して情報の取り扱いに関する誓約書も提出済みであった）

三菱電機の情報管理体制に問題

対策

三菱UFJ銀行と三菱電機の比較

- 三菱電機事案と似た状況がMUFGでも起こり得るのか

	三菱電機	三菱UFJ銀行
攻撃者から狙われ得る重要情報	• 顧客の個人情報 • 従業員の個人情報 • 採用応募者情報 • 退職者の個人情報 • 防衛装備品の設計情報 • 防衛装備品に関する研究試作入札情報 • 防衛装備品の性能要求情報	• 本人情報（氏名，生年月日，性別，住所，電話番号，勤務先 等） • 口座情報 • 生体認証情報（指紋，静脈 等） • 借入金額，借入日，返済状況 • 不渡情報 • 貸付自粛情報
拠点	• 海外拠点 • グループ会社の国内拠点 • グループ会社の海外拠点（中国，イタリア，インド，オーストラリア等）	• 国内の複数拠点 • 海外の支店・出張所 • MUFGグループ（信託，証券，ニコス，アコム，アユタヤ銀行，バンクダナモン等）
起こり得る攻撃の入り口	VPN（本事案における不正アクセスの起点と考えられている）	VPN 不審メール
現状の対策	＜事案発生前＞ • NIST規格「サイバーセキュリティフレームワーク」に則った対策 • 多層防御（挙動検知，制御・監視，バッチ管理，端末の構成一元管理）	• サイバーセキュリティ推進室 • 金融ISACへによる連携 • ログ監視 • 最新の脅威分析 • サイバー演習　　など

三菱UFJ銀行と三菱電機の比較

- 三菱電機事案と似た状況がMUFGでも起こり得るのか

	三菱電機	三菱UFJ銀行
攻撃者から狙われ得る重要情報	• 顧客の個人情報 • 従業員の個人情報 • 採用応募者情報 • 退職者の個人情報 • 防衛装備品の設計情報	• 本人情報（氏名，生年月日，性別，住所，電話番号，勤務先 等） • 口座情報 • 生体認証情報（指紋，静脈 等） • 借入金額，借入日，返済状況
拠点		託，証券，ニコス，行，バンクダナモン
起こり得る攻撃の入り口	考えられている）	不審メール
現状の対策	＜事案発生前＞ • NIST規格「サイバーセキュリティフレームワーク」に則った対策 • 多層防御（挙動検知，制御・監視，バッチ管理，端末の構成一元管理）	• サイバーセキュリティ推進室 • 金融ISACへによる連携 • ログ監視 • 最新の脅威分析 • サイバー演習　　など

三菱電機事案のようにさまざまなセキュリティ対策を講じていても**事前の対策が困難な未公開脆弱性**を狙われることでシステムへの**侵入・感染拡大**は起こり得る．

本事案を踏まえた対策

- **侵入防止**
  - 多要素認証，挙動検知などこれまでの対策
  - ネットワークレベルでのアクセス制御
  - 脆弱性に関する最新情報の収集，脅威分析
- **ファイルレスマルウェアによる感染対策**
  - 不審な添付ファイルを開かない，システムの最新化
- **拡散防止**
  - 拠点間通信のリアルタイム監視・通信遮断
  - 迅速なセキュリティパッチの適用
- **流出防止**
  - 通信遮断の強化
  - 機密性が高い情報の紙ベース，スタンドアロン端末での保管
- **グローバル対応**
  - 海外拠点におけるセキュリティ水準の強化

目次

所感

- ゼロデイ攻撃とファイルレスマルウエアの脅威
  - 対策が難しい面もあるが，リスクを減らすことはできる
- 侵入を前提としたシステムの構築と情報管理
  - どんなに対策をしても高度な攻撃により侵入されてしまうこともある.
  - 侵入検知後に対応できるシステムの構築
  - レジリエントなシステムの構築
  - 取引先との誓約事項を遵守した適切な情報管理（信用に関わる問題）

参考文献

1. 三菱電機，「不正アクセスによる個人情報と企業機密の流出可能性について」，2020年1月20日
2. 三菱電機，「不正アクセスによる個人情報と企業機密の流出可能性について（第2報）」，2020年2月10日
3. 三菱電機，「不正アクセスによる個人情報と企業機密の流出可能性について（第3報）」，2020年2月12日
4. 三菱電機，「不正アクセスによる個人情報と企業機密の流出可能性について（第4報）」，2021年12月24日
5. 防衛省，「三菱電機株式会社に対する不正アクセスによる安全保障状の影響に関する調査結果について」，2021年12月24日
6. piyolog，「ログ消去もされていた三菱電機不正アクセスについてまとめてみた」，2020年2月13日最終更新
7. 時事通信社，「安保情報含む2万件流出か 三菱電機不正アクセス－防衛省」，2021年12月24日
8. 朝日新聞，「VPN 突かれた欠陥」,2020年8月26日朝刊3ページ