令和５年度医療情報セキュリティ研修 及び
サイバーセキュリティインシデント発生時初動対応支援・調査等事業

【はじめに】

今年度のシステム・セキュリティ管理者向け研修について

今年度の研修の構成

※内容は変更する場合がございます。

開催回	カテゴリ	概要	講師
第１回	オリエン	IT環境における組織の管理	萩原 健太 インターバルリンク（株）、(一社)ソフトウェア協会
第２回	基礎	ID管理やアクセス制御 →ITガバナンスと組織管理	村澤 直毅 後藤 昌宏 日本マイクロソフト(株)
第３回		脅威や脆弱性 →アクセス制御とセキュリティ対策	
第４回		効果的なセキュリティの実現	萩原 健太 インターバルリンク（株）、(一社)ソフトウェア協会
第５回	実践	Windows標準機能の活用 →大阪急性期・総合医療センターでの復旧対応	板東 直樹 アップデートテクノロジー(株)、(一社)ソフトウェア協会
第６回		脆弱な機器の守り方 →脆弱な医療機器、サポート切れOSの保護方法について	
第７回		インシデントに備える体制 ログの保護と監視、バックアップ、ネットワーク	

【第7回】システム・セキュリティ管理者向け研修

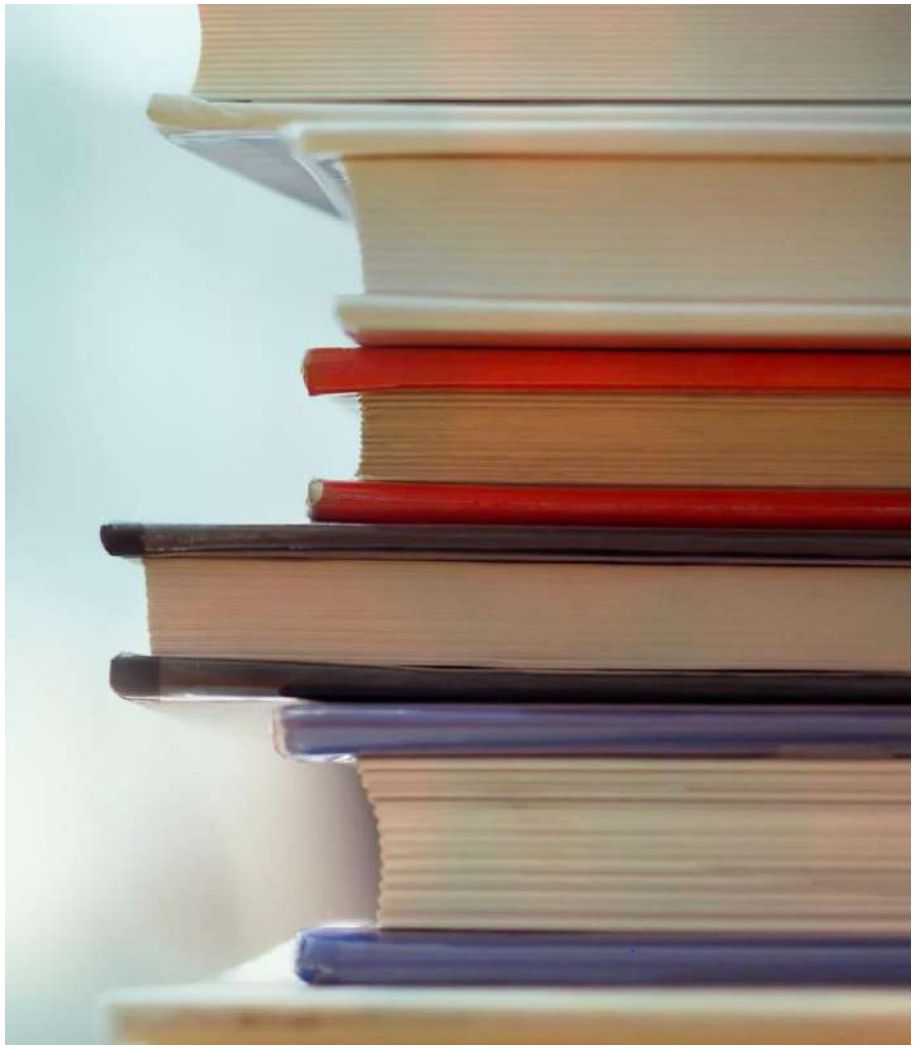
インシデントに備える体制
ログの監視と保護、バックアップ、ネットワーク

2023年12月21日

一般社団法人ソフトウェア協会
板東　直樹

アップデートテクノロジー(株)

本講座の目的



- 本講座では、組織管理のために一般的な管理の基本的な考え方について理解していただき、システム管理責任者もしくはセキュリティ責任者として、ITベンダーと十分なコミュニケーションができる知識とスキルを身につけていただきます。
- ITベンダーと協力しながら、現場でのさまざまな課題を解決することで、円滑なIT運用を行うことを目的としています。

参照すべき資料

- **厚生労働省**
  - 医療情報システムの安全管理に関するガイドライン
  - 医療機関におけるサイバーセキュリティ対策チェックリスト
  - 医療機関におけるサイバーセキュリティ対策チェックリストマニュアル～医療機関・事業者向け～
  - 医療機関における医療機器のサイバーセキュリティ確保のための手引書
- **経済産業省**
  - 医療情報を取り扱う情報システム・サービスの提供事業者における安全管理ガイドライン
- **つるぎ町立半田病院**
  - コンピュータウイルス感染事案有識者会議調査報告書
- **大阪急性期・総合医療センター**
  - 情報セキュリティインシデント調査委員会報告書

第7回のアジェンダ

1. ログの保護と監視
2. バックアップ
3. ネットワーク
4. まとめ

ランサム事案の共通点（弱いところが攻撃されている）

Software Association of Japan

脆弱なネットワーク（初期接続）

VPN装置の接続元制限なし、脆弱性情報の未取得と放置、
公開された資格情報の悪用

弱いパスワード（PCログイン）

5桁、6桁の単純なパスワード
総当たり攻撃、辞書攻撃を許可

管理者権限の付与（ウイルス対策ソフト停止）

アプリケーションの動作を優先
運用テストの設定が放置？

管理者パスワードが共通（資格情報の解析）

運用を優先

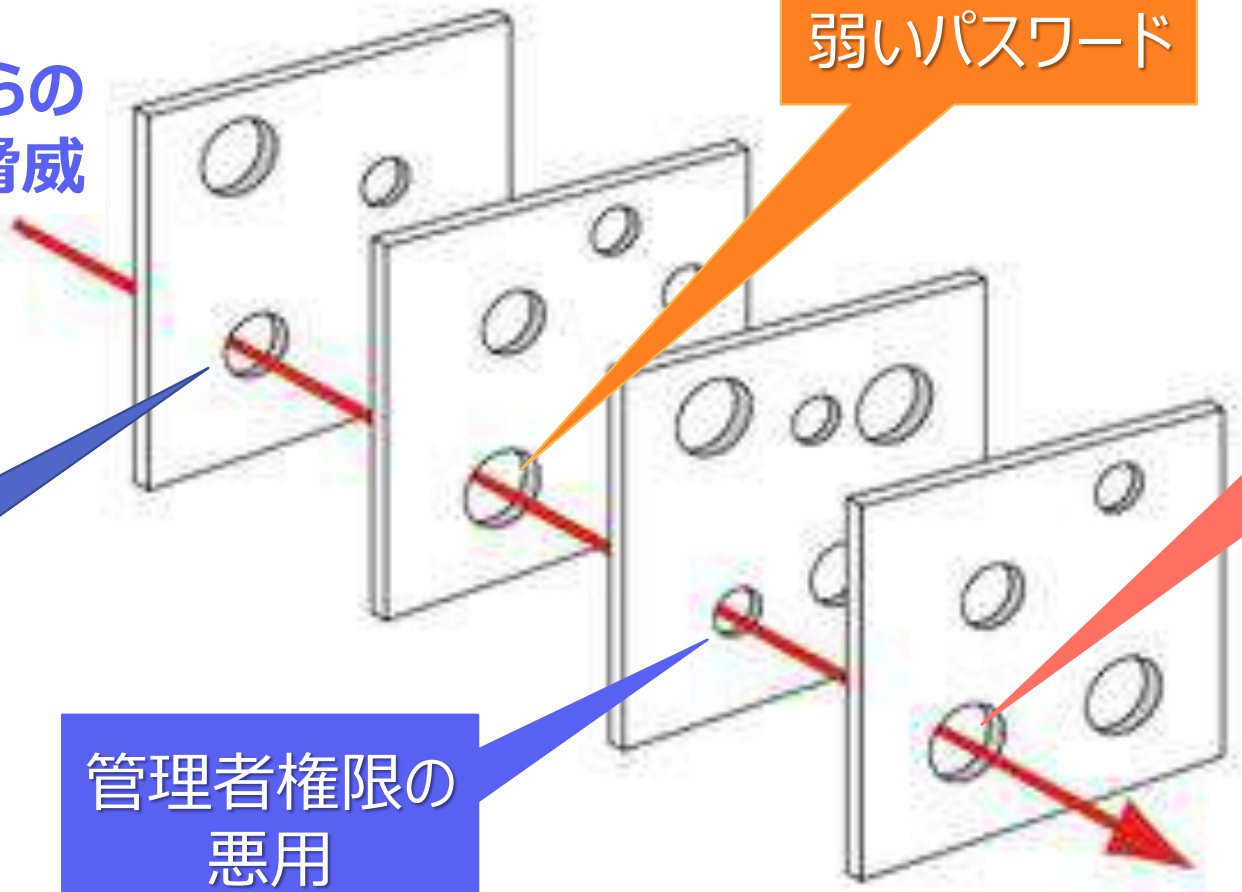
RDP 直接接続（水平展開）

運用を優先

ユーザー権限を管理者権限でなく、標準ユーザーにすれば防御可能であった

第6回セミナー再掲

Swiss Cheese Model



インターネットからの
脅威

脆弱な
弱いパスワード

管理者
パスワードが共通

システムの
脆弱性の放置

管理者権限の
悪用

**水平展開による
サーバーの暗号化、
バックアップの破壊**

第6回セミナー再掲

本来機能すべき防御壁に、**わざわざ穴を空ける設定や運用**が存在している

OGMC で攻撃に使用された PW リスト ①

P@ss2020
P@ssw0rd
P@ssword
p@ssword
P@SSw0rd
p@ssw0rd
P@ss0wrd
P@ss2021
P@ss2022
!qaz@WSx1
admin#DSC2020
admin#DSC
P@ssw0rd123456
P@ssw0rd--
!QAz@wsx3
P@ss@1234
admin
Zaq123
Pass@2022
Admin@123
!qaz@WSx4
123456
123Abc!
P@ssw0rd@2020
Pass@word

P@SSw0rd2022!
P@ssw0rd0
Password@1234
pa$$w0rd
p@ssword01
Pa$$wOrd12
!QAZ@wsx
!QAZ@WSX3
!Qaz@wsx1
Password$1
P@ssw0rd@2019
!qaz@Wsx4
!QAZ@wsx3
P@ssw0rd1
1q2w3e1q3e2w
Passw0rd5
!@12QWqwASas
qwe123QWE
!qaz@WSX4
PassworD123
!qaz@wsx3
1qazxsw2@22
!qaz@wsx
P@$$W0RD
P@ssw0rd@2023

P@ssword1
1q2w3e4r5T
1qaz2wsx
!QAZ@Wsx
!QAZ@wsx4
Passw0rz
P@ssw0rd123
@dmin123
!QAZxsw2
!QAz@wsx1
P@$$w0rd1
1qaz!@#$
!QAZ2wsx
!QAZ@Wsx3
!qaz@Wsx2
!QAZ@Wsx4
abc!@#
1234
1q2w3e4rT
!@#123admin
!Qaz@wsx
!password1
Pa$$word
Qwe123!@#
!@123qwsazx

123456a!
1qaz@WSX
12345678
p@ssword0101
Welcome2020!
Admin@321
!Qaz@wsx3
1qazxsw2@20
qwe123!@#
P@ssw0rd123456
admin#DSC2022
admin@321
!qaz@WSX1
Password888$
1qazxsw2+
admin@123
123qwe!@#
Aa@12356
P@ssword1234
!P@ssw0rd
Passw0rd1
!QAZ@WSX
P@$$w0rd
!qaz@Wsx1
!Qaz@wsx2

!QAz@wsx4
asd@123!@#
Qwer!234
12345
p@ssw0rd!23
Welcome@123
P@ssword123456
P@ssw0rd@2022
P@ssword123
abc123
!qaz@wsx1
1q2w3e4rt
P@assw0rd12345
Pass@1234
P@ssw0rd12345
QAZwsx123
123456A@
P@ssw0rd1234
P@ssw0rd1234567890
P@sswrd
Update@12345
Password@123
P@ssw0rd!
!qaz@wsx4
Passw0rd

ログの監視と保護

とあるコンピュータの Windows Security Log

- **4:07:12 ～ 4:07:22 の10秒間で27回 Event ID 4625 が発生**
- **Event ID4625 = ログオン失敗**

- **短時間に多数のログオン失敗を発生するにはプログラムによる操作が必要**

→プログラムの設定ミス？
ファイル共有で ID/PW を間違った?!

→攻撃ツールの使用？
PWリストからPWを読み込み、
ログオンを試行している?!

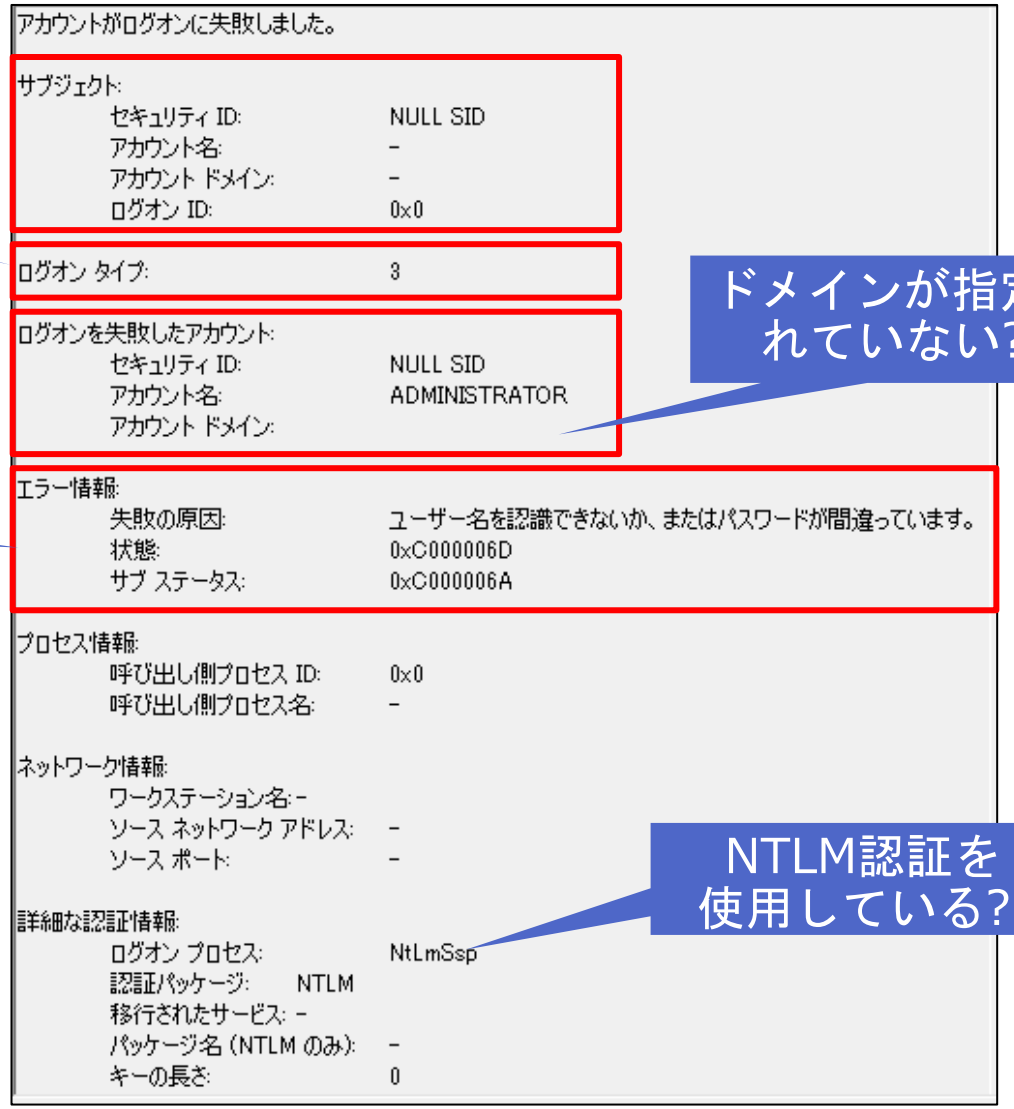
レベル	日付と時刻	ソース	イベント...	タスクのカテゴリ
情報	2022/10/31 3:45:05	Microsoft Windows security auditing.	4625	Logon
情報	2022/10/31 4:07:12	Microsoft Windows security auditing.	4625	Logon
情報	2022/10/31 4:07:13	Microsoft Windows security auditing.	4625	Logon
情報	2022/10/31 4:07:13	Microsoft Windows security auditing.	4625	Logon
情報	2022/10/31 4:07:14	Microsoft Windows security auditing.	4625	Logon
情報	2022/10/31 4:07:14	Microsoft Windows security auditing.	4625	Logon
情報	2022/10/31 4:07:14	Microsoft Windows security auditing.	4625	Logon
情報	2022/10/31 4:07:15	Microsoft Windows security auditing.	4625	Logon
情報	2022/10/31 4:07:15	Microsoft Windows security auditing.	4625	Logon
情報	2022/10/31 4:07:15	Microsoft Windows security auditing.	4625	Logon
情報	2022/10/31 4:07:16	Microsoft Windows security auditing.	4625	Logon
情報	2022/10/31 4:07:16	Microsoft Windows security auditing.	4625	Logon
情報	2022/10/31 4:07:16	Microsoft Windows security auditing.	4625	Logon
情報	2022/10/31 4:07:17	Microsoft Windows security auditing.	4625	Logon
情報	2022/10/31 4:07:17	Microsoft Windows security auditing.	4625	Logon
情報	2022/10/31 4:07:17	Microsoft Windows security auditing.	4625	Logon
情報	2022/10/31 4:07:18	Microsoft Windows security auditing.	4625	Logon
情報	2022/10/31 4:07:18	Microsoft Windows security auditing.	4625	Logon
情報	2022/10/31 4:07:18	Microsoft Windows security auditing.	4625	Logon
情報	2022/10/31 4:07:19	Microsoft Windows security auditing.	4625	Logon
情報	2022/10/31 4:07:19	Microsoft Windows security auditing.	4625	Logon
情報	2022/10/31 4:07:20	Microsoft Windows security auditing.	4625	Logon
情報	2022/10/31 4:07:20	Microsoft Windows security auditing.	4625	Logon
情報	2022/10/31 4:07:20	Microsoft Windows security auditing.	4625	Logon
情報	2022/10/31 4:07:21	Microsoft Windows security auditing.	4625	Logon
情報	2022/10/31 4:07:21	Microsoft Windows security auditing.	4625	Logon
情報	2022/10/31 4:07:22	Microsoft Windows security auditing.	4625	Logon
情報	2022/10/31 4:07:22	Microsoft Windows security auditing.	4625	Logon

Windows Security Log Event ID 4625 の詳細

ログオン失敗を検出したアカウント
記録されない場合がある

ログオン タイプ	種別
2	ユーザーが対話的にログオンした
3	ネットワークからユーザーまたはコンピュータが接続
10	RDP対話型

エラーコード	内容
0xC0000064	スペルミスまたは不適切なユーザー アカウントを使用したユーザー ログオン
0xC000006A	スペルミスまたは不適切なパスワードを使用したユーザー ログオン
0XC000006D	原因は、不適切なユーザー名または認証情報のいずれかです



ドメインが指定されていない?!

NTLM認証を使用している?!

- 通常、プログラムであれば、明示的にドメインを指定すると考えるのが合理的で、その場合は、Kerberos認証になる
- あえて、ドメインを指定しないで Administrator アカウントで、NTLM認証でログオンする理由は何か？

Windows のログオン認証方式

- **Kerberos 認証**
  - MITが開発したネットワーク認証方式で Active Directory の推奨認証方式
  - クライアントとサーバーで相互に認証を行うため、中間者攻撃という、サーバーに成りすました偽サーバーによる ID /パスワードの窃取がない

- **NTLM認証**
  - マイクロソフトが1998年にリリースした古い認証方式 (Windows NT4.0 SP4以降)
    - Active Directory が使用できない Workgroup 環境での認証
    - ファイルサーバー名を指定せず、IP アドレスで指定されたサーバーでの認証
      ¥¥192.168.1.100¥Documents
    - Built-In (コンピュータローカル）のユーザーでログオンする場合
  - 8文字の PW が2.5時間で破られるなど、PW の保存方式に弱点が存在
    - https://www.theregister.com/2019/02/14/password_length/
  - マイクロソフトは Windows 11 24H2、Windows Server 2025 で廃止の予定
    - 今後、NAS の調達では、Kerberos 認証対応について注意が必要

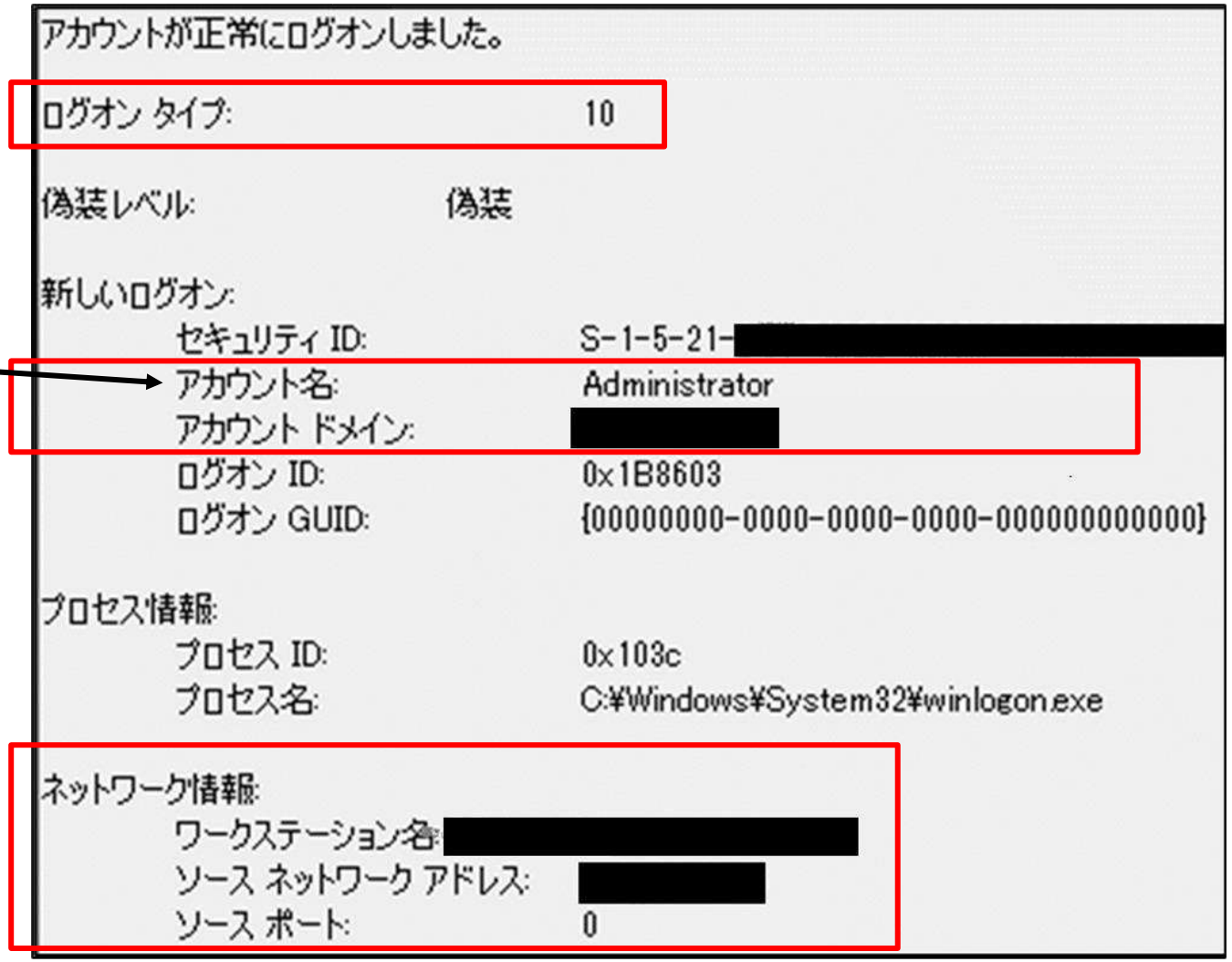
実際には
大阪急性期・総合医療センター (OGMC) が攻撃を受けた際のログ

- **Event ID 4625 アカウントがログオンに失敗しました**
  - 2022/10/31 4:07:12～9:31:20で、1,989 回、給食サーバーで記録されていた
  - OGMC 設置の給食サーバーのBuilt-In Administrator アカウントでログオンを試行
  - バックアップやサーバーにログオンし、暗号化操作と同時並行的に、さらに辞書攻撃を行い、辞書にあるパスワードでログオンできるかを探索していたと考えられる

レベル	日付と時刻	ソース	イベント ID	キーワード
情報	2022/10/31 4:07:23	Microsoft Windows security auditing.	4625	失敗の監査
情報	2022/10/31 4:07:24	Microsoft Windows security auditing.	4625	失敗の監査
情報	2022/10/31 4:07:24	Microsoft Windows security auditing.	4625	失敗の監査
情報	2022/10/31 4:07:24	Microsoft Windows security auditing.	4625	失敗の監査
情報	2022/10/31 4:07:25	Microsoft Windows security auditing.	4625	失敗の監査
情報	2022/10/31 4:07:25	Microsoft Windows security auditing.	4625	失敗の監査
情報	2022/10/31 4:07:26	Microsoft Windows security auditing.	4625	失敗の監査
情報	2022/10/31 4:07:26	Microsoft Windows security auditing.	4625	失敗の監査
情報	2022/10/31 4:07:26	Microsoft Windows security auditing.	4625	失敗の監査
情報	2022/10/31 4:07:27	Microsoft Windows security auditing.	4625	失敗の監査
情報	2022/10/31 4:07:27	Microsoft Windows security auditing.	4625	失敗の監査
情報	2022/10/31 4:07:27	Microsoft Windows security auditing.	4625	失敗の監査
情報	2022/10/31 4:07:28	Microsoft Windows security auditing.	4625	失敗の監査
情報	2022/10/31 4:07:28	Microsoft Windows security auditing.	4625	失敗の監査
情報	2022/10/31 4:07:29	Microsoft Windows security auditing.	4625	失敗の監査
情報	2022/10/31 4:07:29	Microsoft Windows security auditing.	4625	失敗の監査
情報	2022/10/31 4:07:29	Microsoft Windows security auditing.	4625	失敗の監査
情報	2022/10/31 4:07:30	Microsoft Windows security auditing.	4625	失敗の監査
情報	2022/10/31 4:07:30	Microsoft Windows security auditing.	4625	失敗の監査
情報	2022/10/31 4:07:30	Microsoft Windows security auditing.	4625	失敗の監査
情報	2022/10/31 4:07:31	Microsoft Windows security auditing.	4625	失敗の監査
情報	2022/10/31 4:07:31	Microsoft Windows security auditing.	4625	失敗の監査
情報	2022/10/31 4:07:31	Microsoft Windows security auditing.	4625	失敗の監査
情報	2022/10/31 4:07:32	Microsoft Windows security auditing.	4625	失敗の監査
情報	2022/10/31 4:07:32	Microsoft Windows security auditing.	4625	失敗の監査
情報	2022/10/31 4:07:33	Microsoft Windows security auditing.	4625	失敗の監査
情報	2022/10/31 4:07:33	Microsoft Windows security auditing.	4625	失敗の監査
情報	2022/10/31 4:07:33	Microsoft Windows security auditing.	4625	失敗の監査
情報	2022/10/31 4:07:34	Microsoft Windows security auditing.	4625	失敗の監査

攻撃者の侵入成功時のログ

- **Event ID 4624 アカウントがログオンに成功しました**
  - 2022/10/31 4:07:14
  - ログオンタイプ：10 (RDP)
  - アカウント名：Administrator
  - アカウントドメイン：サーバー名
  - ネットワークアドレス：
    給食事業者のサーバーの IP アドレス



フォレンジック調査に役立つ Windows ログ

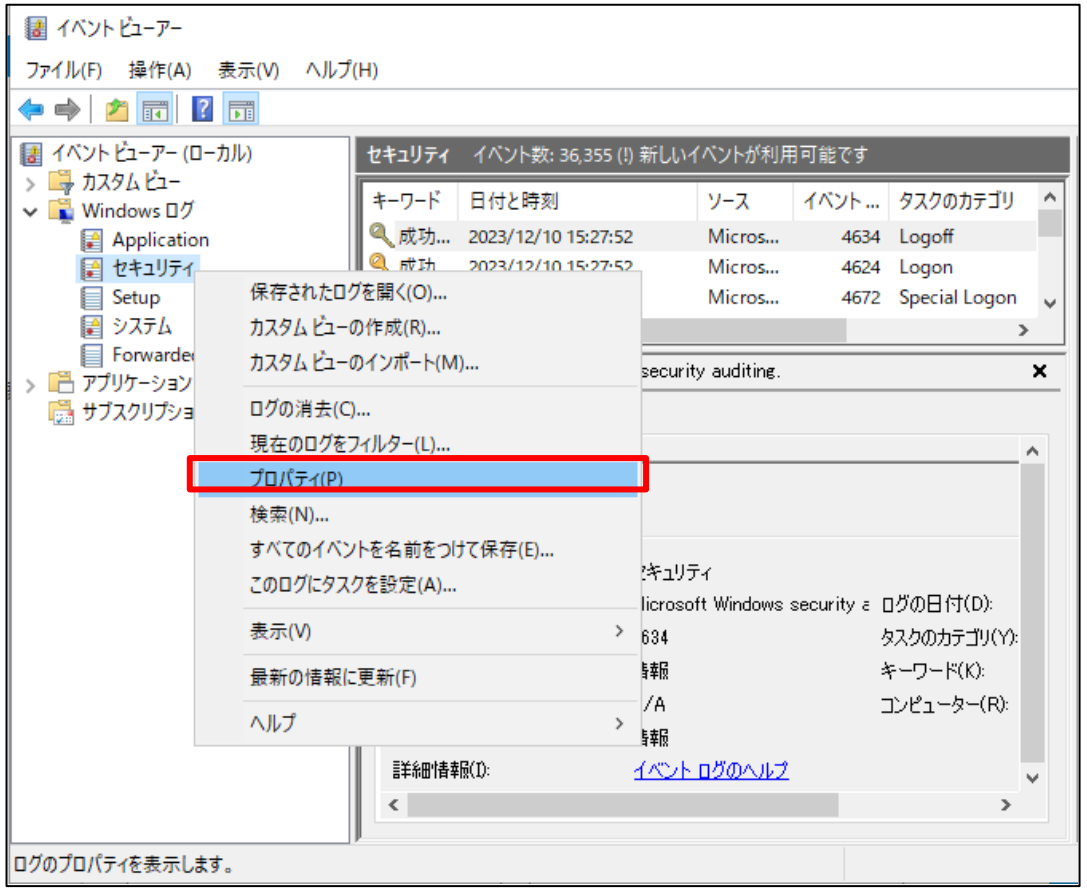
ログ名称	内容	推奨サイズ(KB)
[Windows ログ]>[Application]	アプリケーションのインストール、ウイルス対策ソフトの設定変更等	20,000 以上
[Windows ログ]>[セキュリティ]	ログオン失敗、成功、セキュリティグループの変更等	40,000 以上
[Windows ログ]>[システム]	再起動、サービス停止、レジストリ変更等	20,000 以上
[アプリケーションとサービスログ]>[Microsoft]>[Windows]>[Microsoft-Windows-SmbClient%4Security.evtx] もしくは [SMBServer]>[Client]	SMB ファイル共有　（クライアント）	20,000 以上
[アプリケーションとサービスログ]>[Microsoft]>[Windows]>[Microsoft-Windows-SMBServer/Security.evtx] もしくは [SMBServer]>[Security]	SMB ファイル共有　（サーバー）	20,000 以上

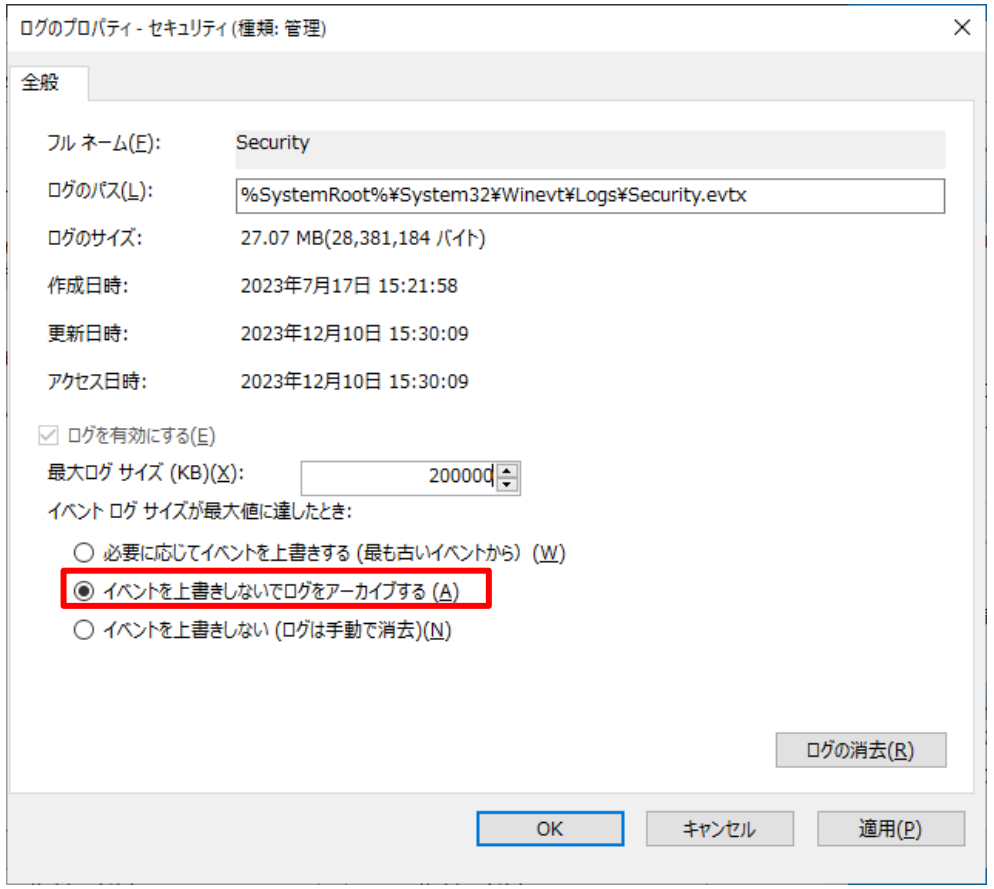
フォレンジック調査に役立つ Windows ログ

ログ名称	内容	推奨サイズ(KB)
[アプリケーションとサービスログ]>[Microsoft]>[Windows]>[Microsoft-Windows-TerminalServices-LocalSessionManager/Operational.evtx] もしくは [TerminalServices-LocalSessionManager]>[Operational]	RDP接続	20,000 以上
[アプリケーションとサービスログ]>[Microsoft]>[Windows]>[Microsoft-Windows-TerminalServices-RDPClient/Operational.evtx] もしくは [TerminalServices-ClientActiveXCore]>[Microsoft-Windows-TerminalServices-RDPClient/Operational]		20,000 以上

- Event ログの保存場所：C:¥Windows¥System32¥winevt¥Logs
- サイズの設定方法: 次頁参照

[イベントビューワー]>[セキュリティ]>[プロパティ]





- サーバーマネージャーで [イベントビューワー] を起動し、設定するログを右クリックする
- Cドライブの空き容量がひっ迫している場合は、[必要に応じてイベントを上書きする] を選択する

OGMC 給食サーバーの Application ログ

Timestamp	Channel	Summary
2022-10-31T04:17:33.0000000	Application	Windows インストーラー トランザクションを開始しています: C:\Users\ADMINI~1\AppData\Local\T
2022-10-31T04:18:04.6044121	Application	セッション 0 - 2022-10-30T19:18:04.6044121００Z を起動しています。
2022-10-31T04:18:05.0000000	Application	Product: Advanced IP Scanner 2.5.1 -- Installation completed successfully.
2022-10-31T04:18:05.0000000	Application	Windows インストーラーにより製品がインストールされました。製品名: Advanced IP Scanner 2.5.1。
2022-10-31T04:18:05.0000000	Application	Windows インストーラー トランザクションを終了しています: C:\Users\ADMINI~1\AppData\Local\T

- **攻撃者に悪用された Advanced IP Scanner のインストールの痕跡**
  - 指定した範囲のIPアドレスをスキャンして、ネットワーク上のコンピュータを検出する無償のソフトウェア
  - RDP接続 (3389/TCP) 可能なコンピュータも検出できる
  - Wake-On-LAN、リモートシャットダウンなども可能
  - 一般的な製品なので、ウイルス対策ソフトでは駆除されない

給食サーバーのデスクトップにあった攻撃ツール

PW 解析ツール
Mimikatz

RDP ポートの
調査ツール

MIMIx64	2022/10/31 4:16	ファイル フォルダー	
Advanced_IP_Scanner_2.5.4594.1.exe	2022/08/23 23:48	アプリケーション	20,558 KB
credentials.txt	2022/10/31 4:22	テキスト ドキュメント	23 KB
good.txt	2022/10/31 4:22	テキスト ドキュメント	26 KB
ip.txt	2022/10/31 4:21	テキスト ドキュメント	5 KB
passwordupdate.txt	2022/10/31 4:05	テキスト ドキュメント	3 KB
servers.txt	2022/10/31 4:49	テキスト ドキュメント	6 KB
settings.ini	2022/10/31 4:49	構成設定	1 KB
user.txt	2022/10/31 4:05	テキスト ドキュメント	1 KB

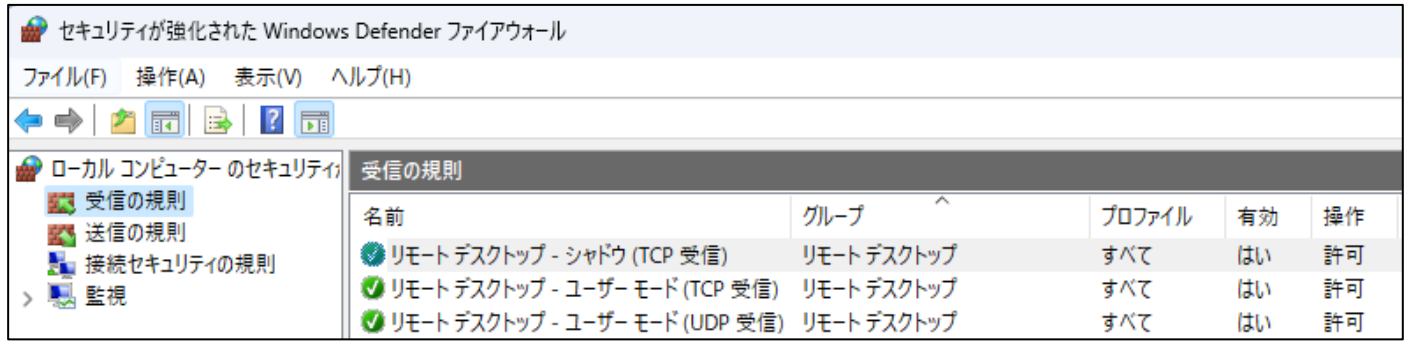
攻撃初期に分析するべき RDP 関連 Log

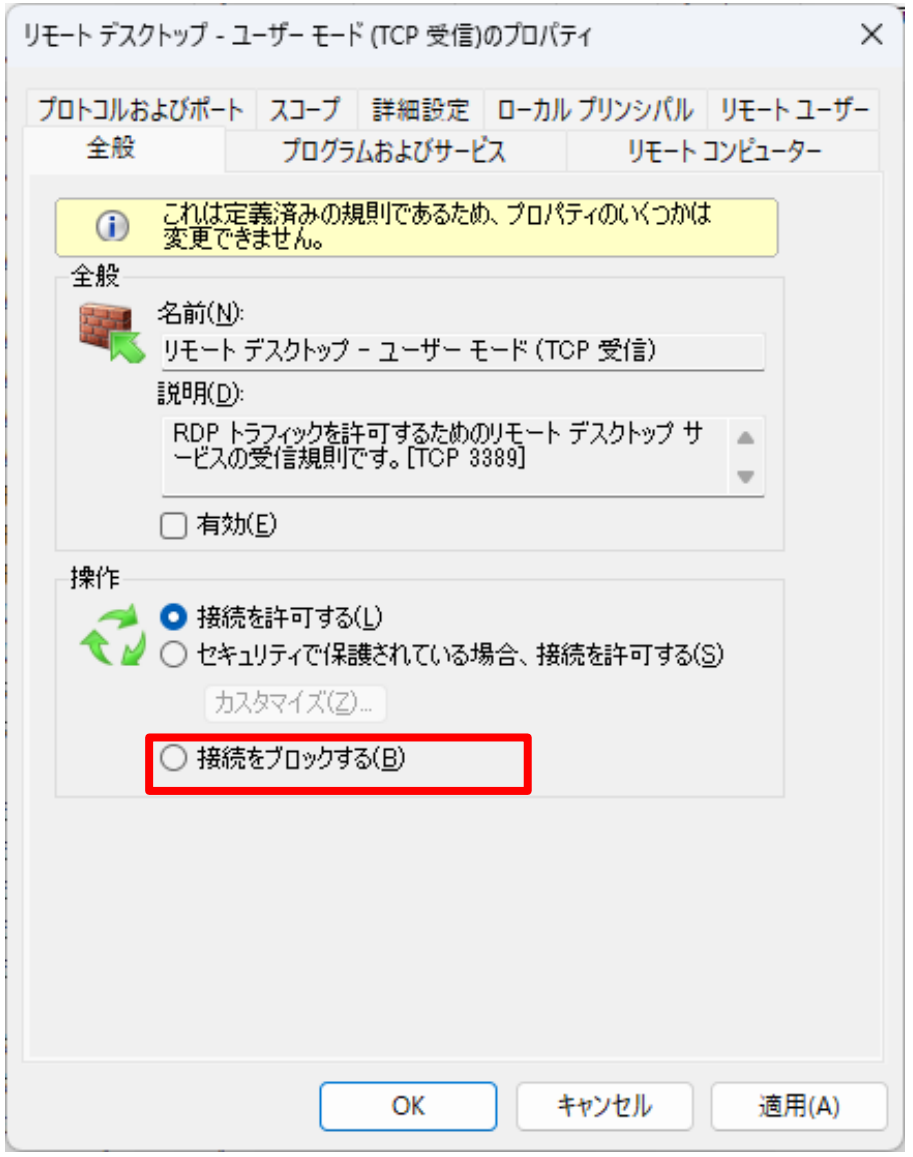
- **Microsoft-Windows-TerminalServices-LocalSessionManager%4Operational.evtx**
  - Event ID 21 と同時刻の Security ログの Event ID 4624 の双方を調べる
  - 4624 ログオン成功がある場合、そのユーザー名、ソースネットワークアドレスから不審な RDP ログオンがないかを調べる
  - ソースネットワークアドレスがローカルの場合は、ローカルログオンであり、RDP接続ではないことに注意する

- **Microsoft-Windows-TerminalServices-RDPClient/Operational (TerminalServices-ClientActiveXCore)**
  - Event ID 1102 で接続先の IP アドレスが確認できる

- **定期的にこれらを調査し、想定外の不審な RDP 接続がないことを確認する**
  - RDP 接続されるサーバー、使用するアカウント、接続元アドレスの一覧を作成しておく
  - 異常があれば、ネットワークを抜線 or パーソナルFirewall で RDP 3389 を無効にし、セキュリティベンダーに相談する（次頁詳細）

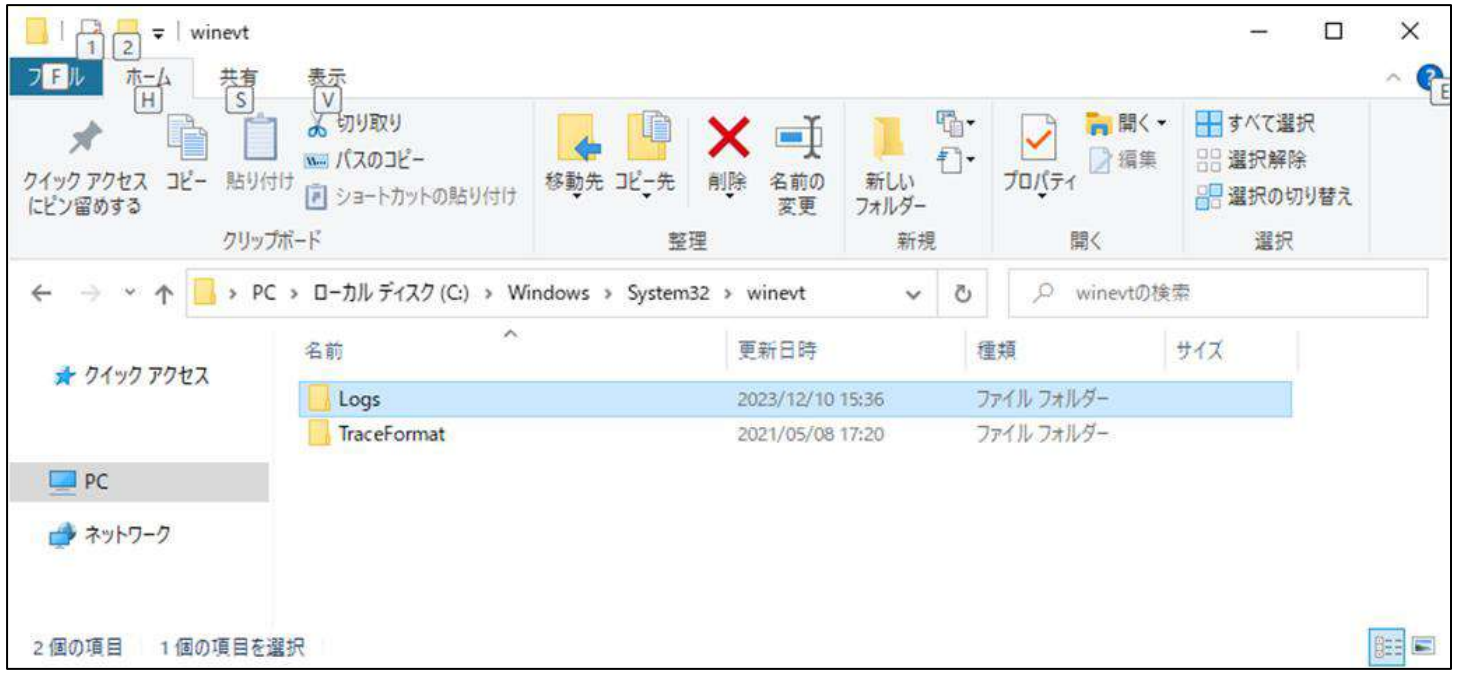
RDP Firewall での無効化

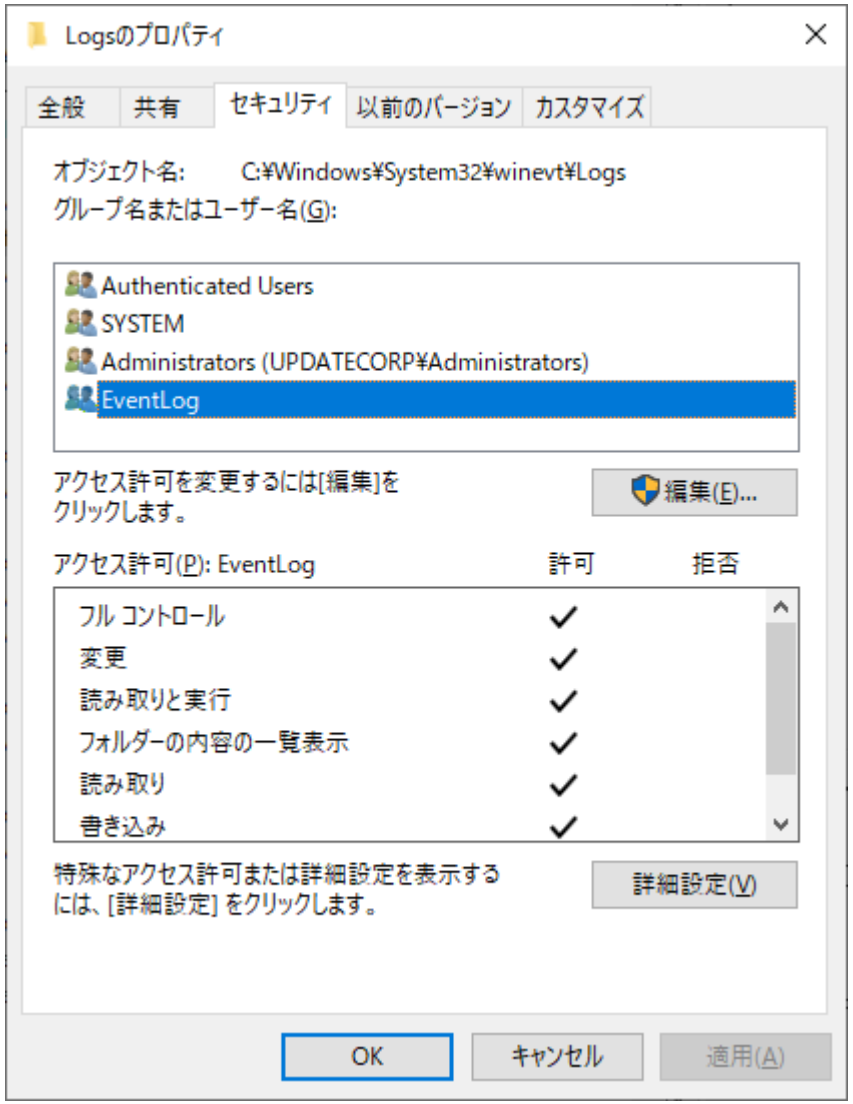




ログの保護

- **C:¥Windows¥System32¥Logs**
  - 右クリックし、Logs のプロパティからセキュリティを選択
  - Eventlog、SYSTEM、Domain¥Administrators が [フルコントロール] となっていることを確認する

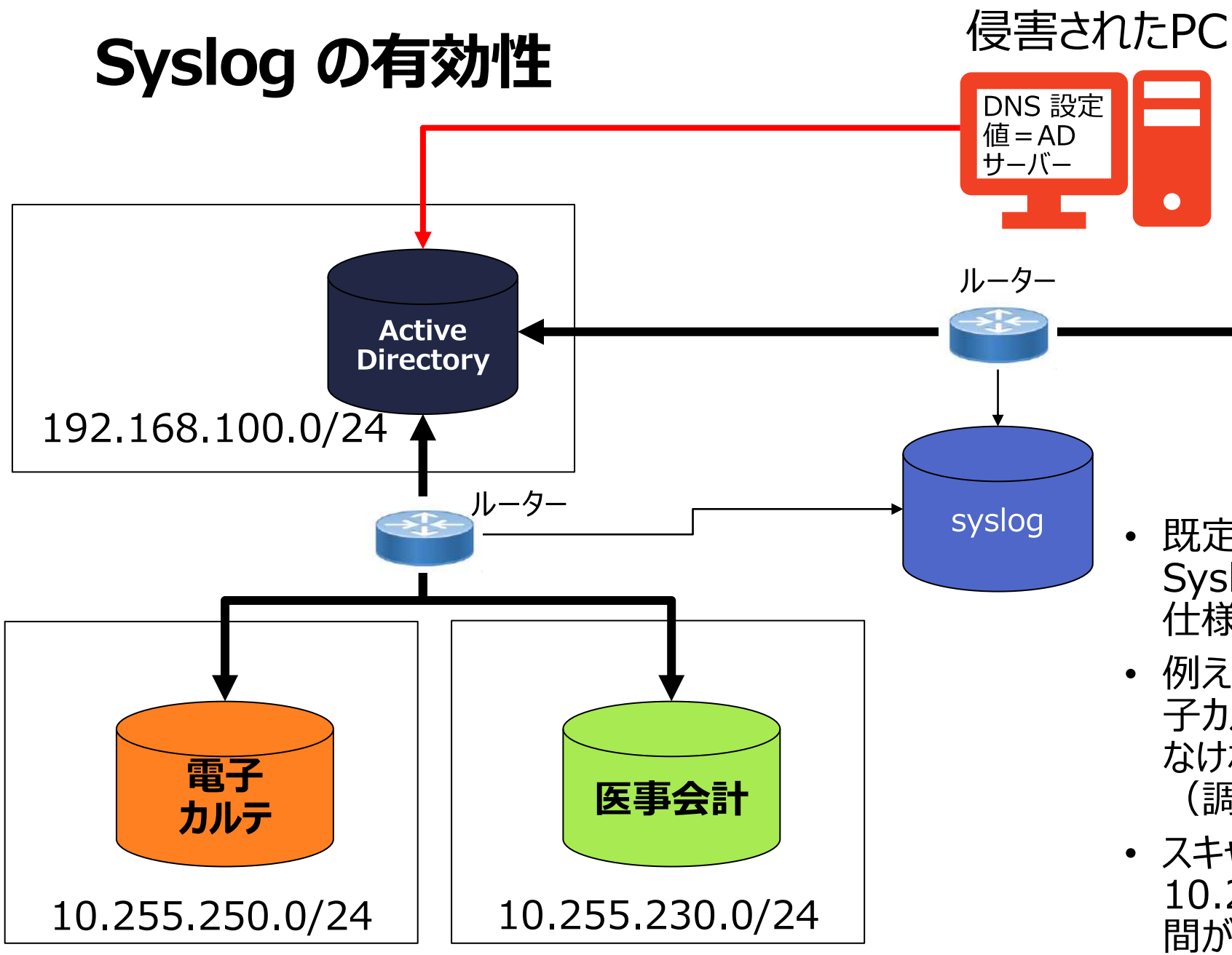




Windows ログでの検出の限界

- **Windows ログはセキュリティ違反検出用ではない**
  - Windows 開発における Debug 用に近く、ログだけですべてが分かる訳ではない
  - CPU 負荷が高いと、すべての事象が 100% 記録されるわけではない
  - 攻撃者は、管理者権限を取得して、ログを消去することもある
  - 4625 などが常時多発しているような環境では、攻撃なのか、設定ミスなのか判別がつかなくなる
    - 4625 が多い場合は、ベンダーに原因解消を求める
- **Firewall や、ネットワークセグメント用ルーターの Syslog が重要**
  - Windows ログと併せて分析に役立つ
  - 特にセグメント分割のためのルーター、L3スイッチの Syslog 取得は、水平展開があったかを知ることができ、攻撃範囲の特定に役立つ
  - Firewallやルーター本体に保存せず、Syslog サーバーへの転送や、USBメモリ等へ保存する
    - 真正性の証明に役立つ
    - 早期復旧に資する

Syslog の有効性



- 既定ではルーター本体に保存される Syslog を専用サーバーに保管する設定を仕様書で求めておく
- 例えば、インシデント発生時に AD から電子カルテへの RDP 接続や SMB 接続がなければ、侵害されてない可能性が高まる（調査範囲が狭まる＝復旧が早くなる）
- スキャナーで10.0.0.0 から 10.255.230.0 まで調べるには相当の時間がかかり、諦める可能性も高まる

バックアップ

医療法等による文書の法定保存期間

書類			法定保存期間	根拠法令		
診療録			最終記載日から5年	医師法第24条、歯科医師法第23条		
			その完結の日から５年	保険医療機関及び保険医療養担当規則第９条		
医薬品関連	指定再生医療等製品を使用した記録		最終使用日から20年	医療法施行規則第14条	医薬品医療機器等法施行規則	第228条の19
	特定生物由来製品を使用した記録					第240条
	麻薬	麻薬譲渡証	交付又は提供の日から2年	麻薬及び向精神薬取締法	第32条	
		麻薬管理帳簿	最終記載日から2年		第39条	
	向精神薬	第1種・第2種向精神薬の管理帳簿	記録の日から2年		第50条の23	
	覚醒剤原料	覚醒剤原料譲渡証	譲渡の日から2年	覚醒剤取締法	第30条の10	
		覚醒剤原料の管理帳簿	最終記載日から2年		第30条の17	
診療用放射線関連	エックス線装置等の測定結果記録		5年	医療法施行規則	第30条の21	
	放射線障害が発生するおそれのある場所の測定結果記録				第30条の22	
	エックス線装置等の使用時間に関する帳簿		閉鎖後2年		第30条の23	
	診療用放射線照射装置等の入手・使用・廃棄等に関する帳簿		閉鎖後5年			
助産録			5年	保健師助産師看護師法第42条		
歯科衛生士業務記録			3年	歯科衛生士法施行規則第18条		
歯科技工指示書			歯科技工終了日から2年	歯科技工士法第19条		

バックアップの基本的な考え方

- **攻撃者の視点**
  - 攻撃者は身代金獲得のためにバックアップを破壊する
  - サーバーに侵入された時点で、サーバーのバックアップエージェントの設定を取得し、バックアップの所在は知られてしまう
- **バックアップの 3-2-1 ルール**
  - 3 つのバックアップデータをコピー
  - 2 つの異なるメディアへコピー
  - 1 つはオフサイト保管
    もしくは
    イミュータブル（作成後にその状態を変えることのできない）、ライトワンスストレージ
- **バックアップのネットワーク**
  - サーバー群にバックアップがあると、すぐに発見されてしまう
  - クラウド化、もしくは、異なるネットワークセグメントに保存することを検討する（後述）

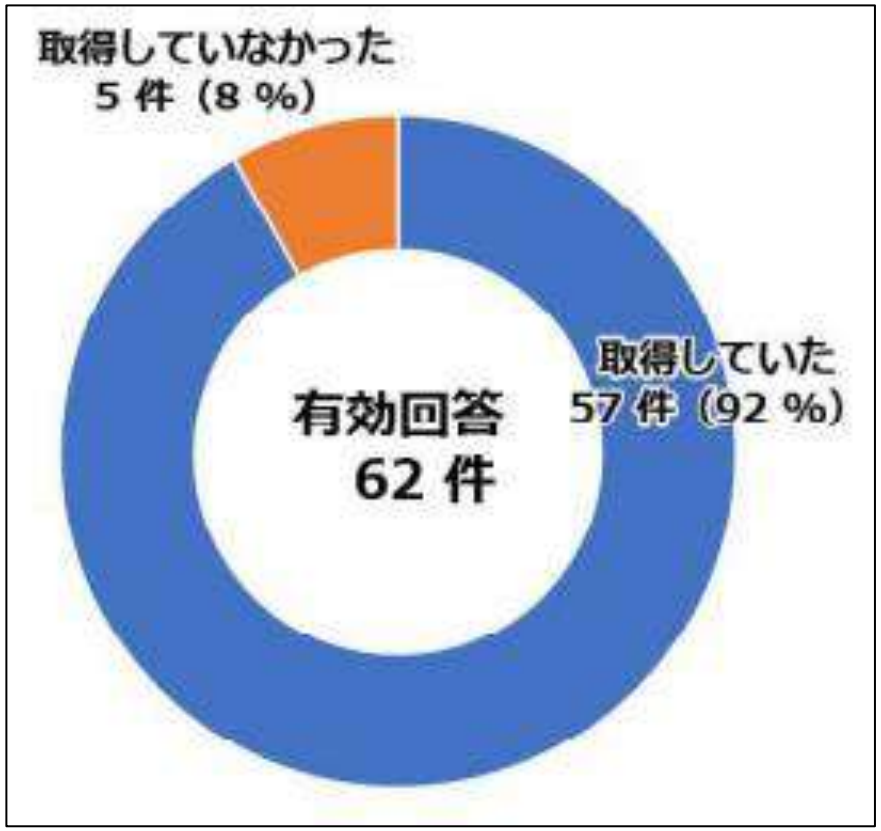
取得しておくべきバックアップ

- **電子カルテ、医事会計、部門・診療系システムのシステムのバックアップ**
  - 感染時にすぐにバックアップからの参照系を立ち上げるために準備する
  - 端末のシステムもバックアップを取得しておく
  - 新規構築した際に、取得するよう仕様書で要求しておく
    - 多くのベンダーは復旧経験に乏しいため、仕様書では、実際の復旧テスト報告書作成も要件に入れておく

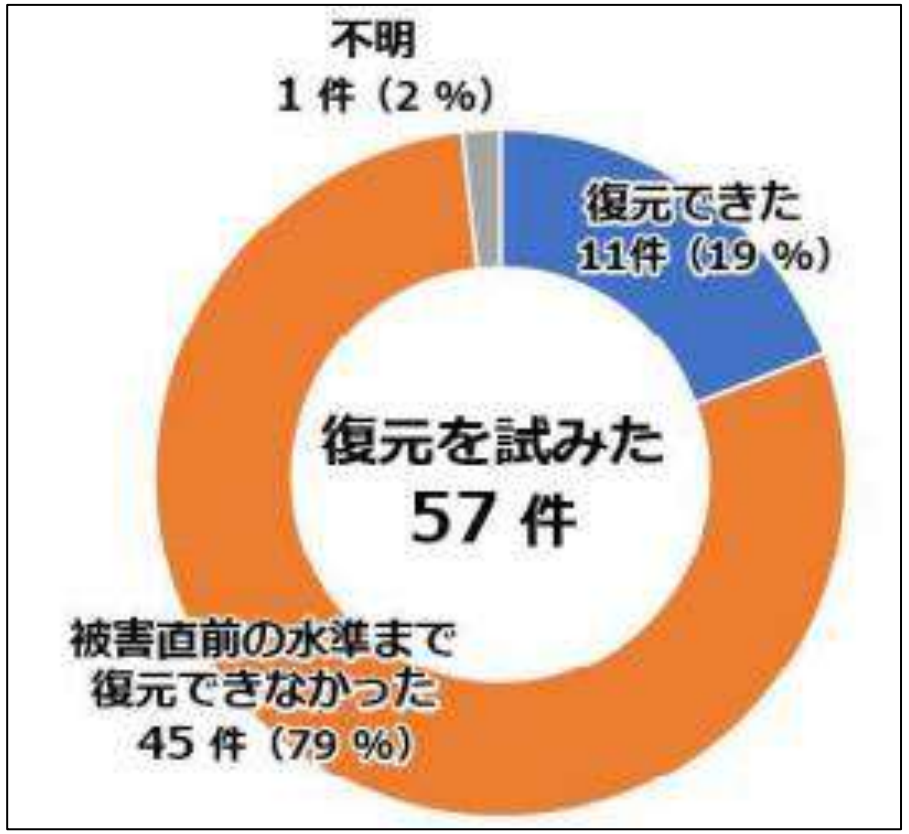
- **ワープロ端末のイメージバックアップ**
  - 紙カルテ運用では、字が汚く、インシデントにつながる
  - 特に「カタカナ」は、取り違えの原因になるため、ワープロ端末の早期立ち上げが重要
    - シ → ツ、ジ → ヅ、
  - このため、Windows ＋ワープロソフト＋プリンタドライバをインストールした状態の、イメージバックアップを準備しておく

令和５年上半期における
サイバー空間をめぐる脅威の情勢等について（警察庁）

バックアップ取得の有無



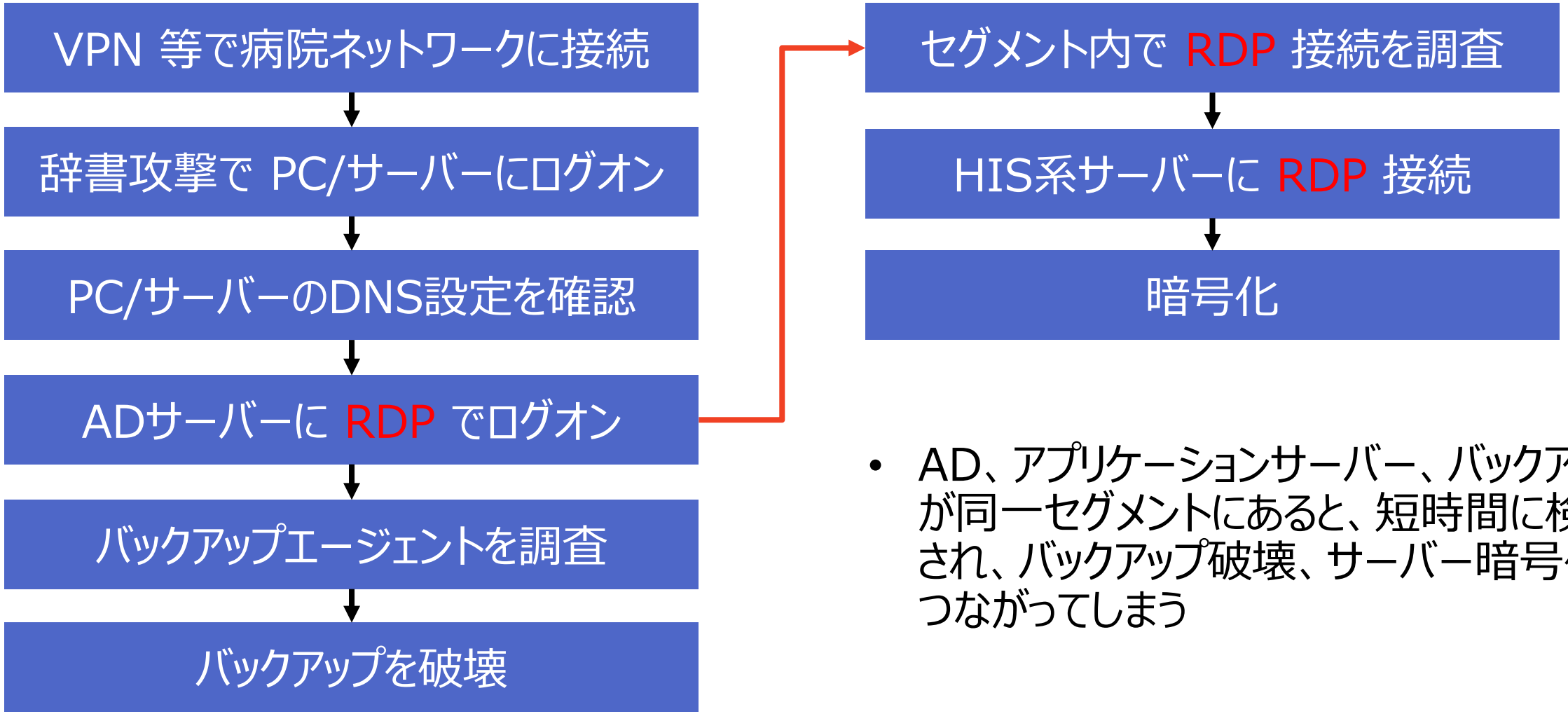
バックアップからの復元結果



https://www.npa.go.jp/publications/statistics/cybersecurity/data/R05_kami_cyber_jousei.pdf

ネットワーク

攻撃者の手口



- AD、アプリケーションサーバー、バックアップが同一セグメントにあると、短時間に検出され、バックアップ破壊、サーバー暗号化につながってしまう

ルーティングで特に注意すべきポート

第6回セミナー再掲

カテゴリー	プロトコル・ポート番号
リモートアクセス	RDP (3389)、SSH (22)、Telnet (23)
ファイル転送/ファイル共有	FTP (20、21)、SMB (139、445)
プロセス間通信	RPC (135)、NetBIOS (137、138、139)、SNMP (161、162)
認証	Kerberos (88、464)、LDAP (389)、LDAPS (636)、
データベース	SQL Server (1433)、Oracle (1521)

■ ランサムウェア事案では、大半が RDP を悪用するため、RDPの規定のポートである3389を他のポートに設定することを検討する。（レジストリ設定の場合）

Registry Hive	HKEY_LOCAL_MACHINE
Registry Path	System¥CurrentControlSet¥Control¥Terminal Server¥WinStations¥RDP-Tcp
Value Name	PortNumber
Value Type	REG_DWORD
Value	49152から65535 までのいずれかを指定する（10進)

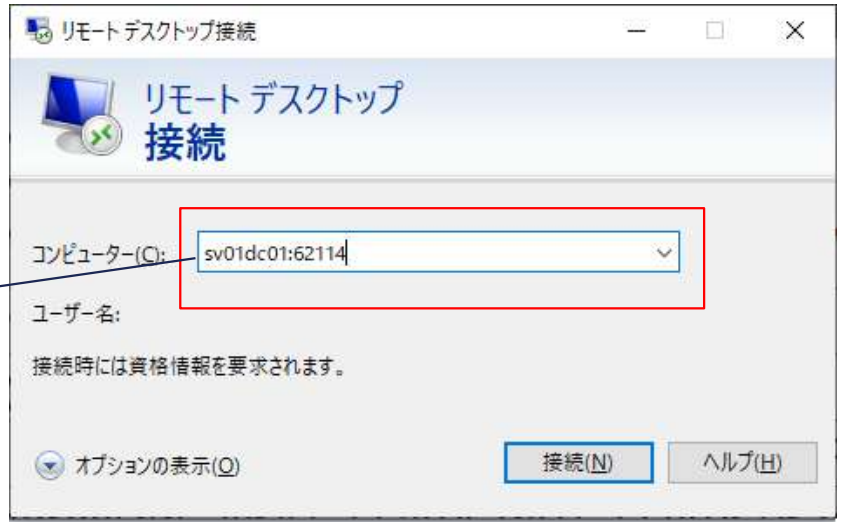
■ 既定では、¥Terminal Server¥WinStations¥RDP-Tcp というキーは存在していないので、作成する。

PowerShell による RDP ポートの変更

第6回セミナー再掲

- **PowerShell を管理者モードで起動し、以下のコマンドを実行する**
  - $portvalue = 62114
  - Set-ItemProperty -Path 'HKLM:¥SYSTEM¥CurrentControlSet¥Control¥Terminal Server¥WinStations¥RDP-Tcp' -name "PortNumber" -Value $portvalue
    (すべて一行)
  - パーソナル Firewall で「受信の規則」>「リモートデスクトップ」 >「ユーザーモードTCP受信」、「ユーザーモードUDP受信」のローカルポートを 62114 に変更する
  - サーバー名の後ろに ":" を付けて設定したポート番号を指定する

SV01dc01:62114

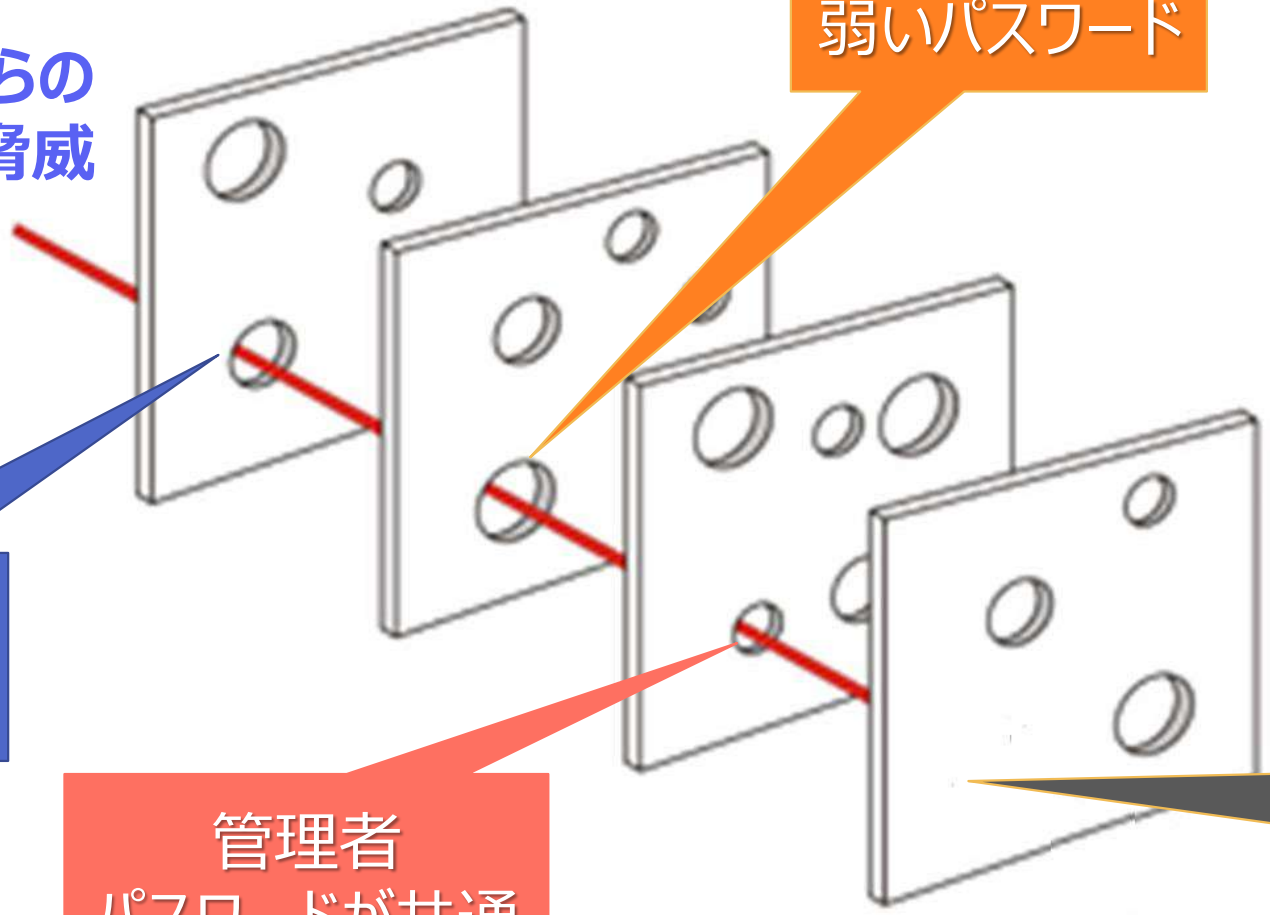


攻撃に対抗するためのネットワーク構成の考え方

- **Active Directory サーバーと HIS 系サーバーのネットワーク分離を仕様に含める**
  - AD、HIS系サーバー、PACS、バックアップを異なるセグメントに配置し、同じセグメントにはおかない
  - 各セグメント間は、必要最小限のルーティング設定を行う
    - セグメントを分けていても、ルーティング制限がないフラットな設定が多いことに留意
  - 電子カルテ、医事会計、オーダリング、看護支援等の基幹システムのバックアップはオフライン、イミュータブル、ライトワンスのいずれかを選択する
    - 各システムが使用できない場合のダメージを、各部門、事務局を交え検討する
- **分離のメリット**
  - 水平展開を局所化し、早期復旧につながる
    - ポートスキャンツールを使用しても、検出に時間がかかる
    - 調査に時間がかかり、AD だけの被害で収まる可能性が高まる
  - セグメント間のルーター、L3スイッチで Syslog を取得する
    - ツールのログから、侵害を受けていない＝真正性が担保されていることの証明となる

Swiss Cheese Model

インターネットからの
脅威



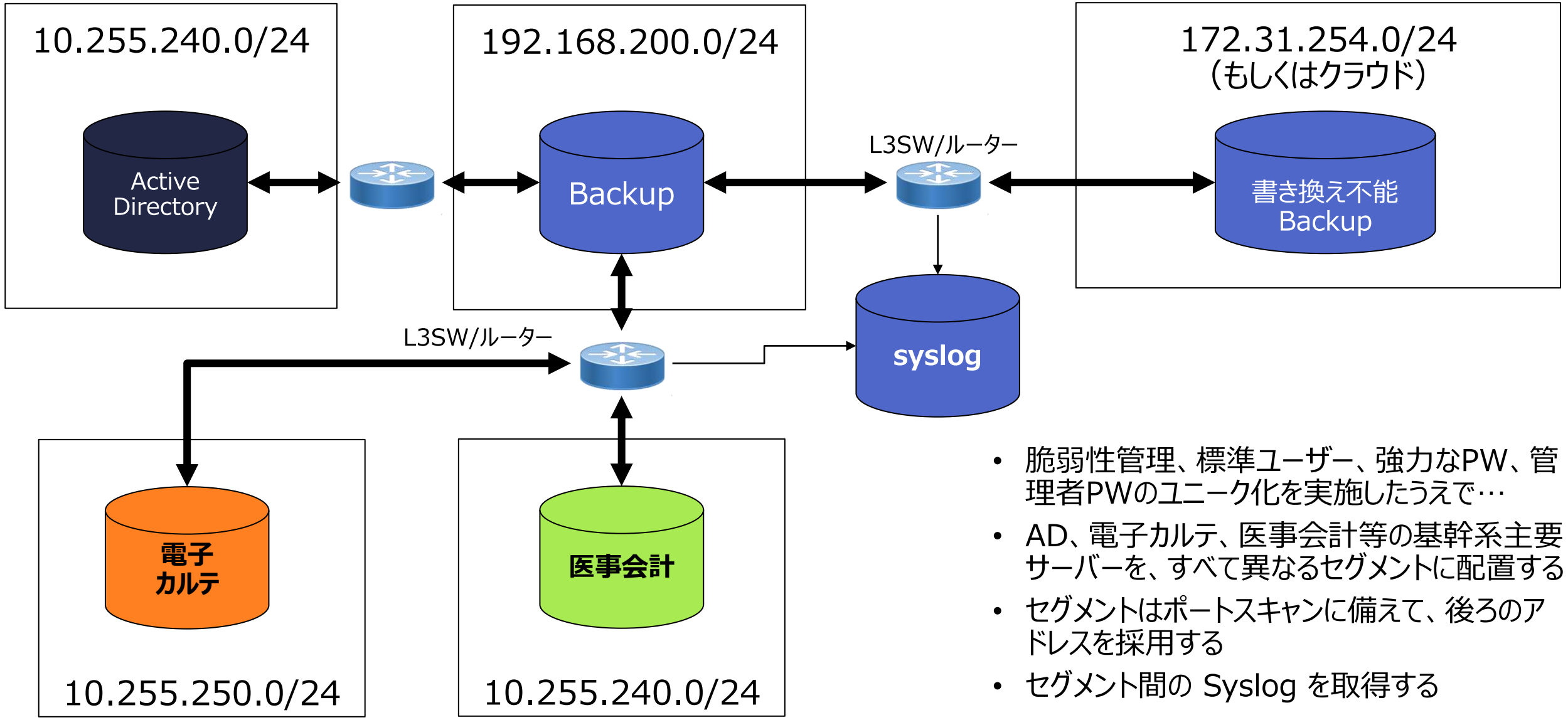
脆弱な
弱いパスワード

システムの
脆弱性の放置

管理者
パスワードが共通

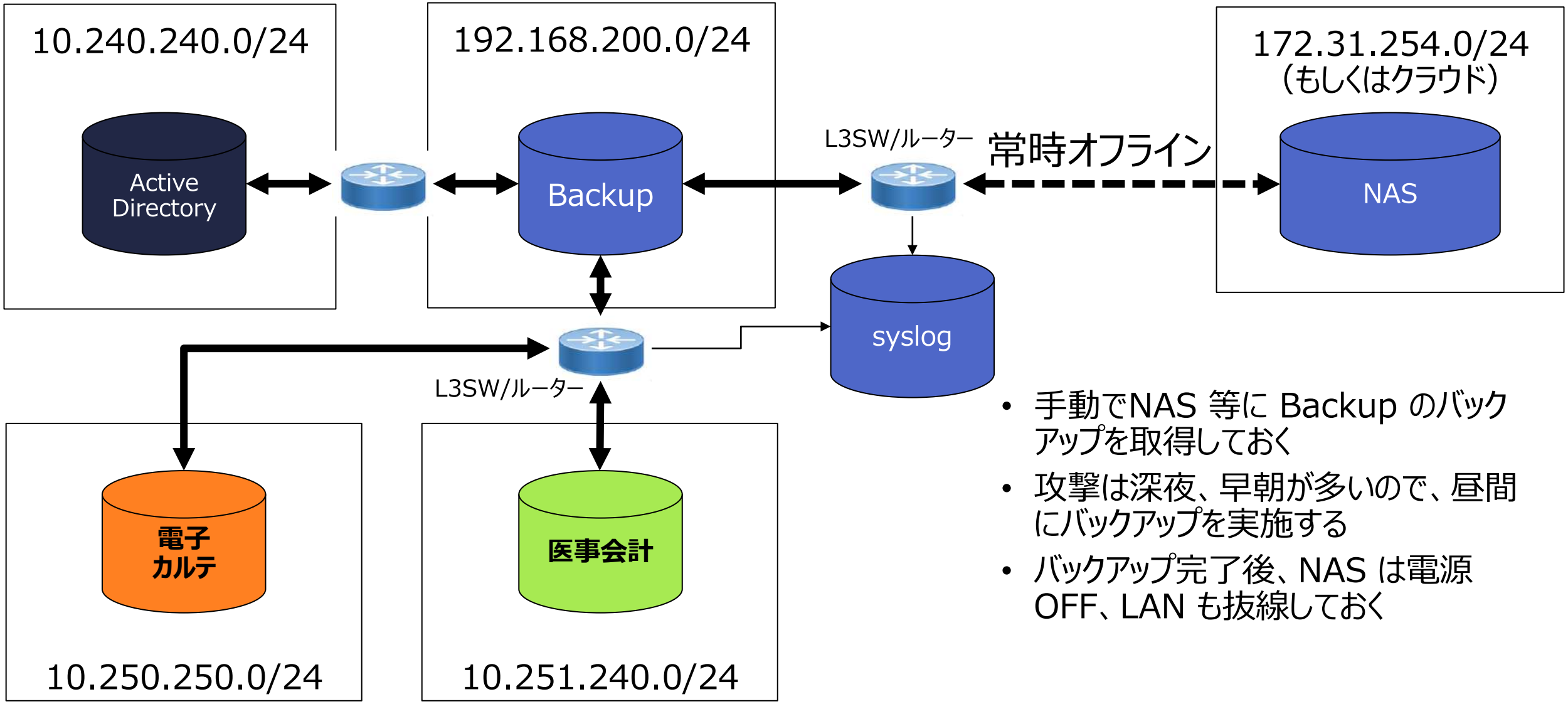
ネットワーク構成と
RDP 設定変更で
局所化する

ランサム攻撃に強いネットワーク構成例



- 脆弱性管理、標準ユーザー、強力なPW、管理者PWのユニーク化を実施したうえで…
- AD、電子カルテ、医事会計等の基幹系主要サーバーを、すべて異なるセグメントに配置する
- セグメントはポートスキャンに備えて、後ろのアドレスを採用する
- セグメント間の Syslog を取得する

ランサム攻撃に強いネットワーク構成（小規模施設）



- 手動でNAS 等に Backup のバックアップを取得しておく
- 攻撃は深夜、早朝が多いので、昼間にバックアップを実施する
- バックアップ完了後、NAS は電源 OFF、LAN も抜線しておく

EDR、セキュリティ製品に関する考え方

- **EDR、セキュリティ製品は万能ではない**
  - ランサム攻撃集団は、様々なセキュリティ製品を購入し、検出されないための工夫を重ねている
    - 「こんにちは、2 つのアンチウイルスを他のアンチウイルスに置き換えることは可能ですか？ CrowdStrike について話しているのですが、実際、彼らは営業担当者を通じてオフラインでのみライセンスを販売しています。私は彼らに連絡しました。月曜日、昨日メールに書いたのですが、今のところ返事がありません。どうしても購入できない場合は、トライアルで再度アクティベートを試みますが。 Crowdstrike は別として、トレンドマイクロだけが残っており、残りはすでにディフェンダーに送られています。」
    - 「彼が言う唯一のことは、一部の AV がブロックされているということです。現在、トレンドマイクロと ESET からの検出除外を行っています。」「トレンドマイクロとウェブブリュットはウイルスを発見しませんでしたか？」「トレンドマイクロとウェブルートは間違いなく検出している」
- **多層防御の一つのパーツ**
  - バックアップの秘匿、ネットワーク構成の変更、Windows の強化設定等の一部として使用し、全面的に依存しない
  - 管理者権限や脆弱性があれば、**Uninstall** されてしまう可能性がある

出典：三井物産セキュアディレクション ContiLeaks の概要まとめ Rev.3
https://www.mbsd.jp/2022/03/08/assets/images/MBSD_Summary_of_ContiLeaks_Rev3.pdf

まとめ

- **ログ**
  - ログオン失敗 Security ログ Event ID 4625
    - 1秒間に数回連続し、かつ長時間にわたる場合は、アカウントとソースIPアドレスから、攻撃か、設定ミスかを切り分けて行動する、異常が疑われたら RDP を停止
  - SMB、RDP、Application のログは、調査に重要
  - Firewall、ルーター、L3スイッチの Syslog は被害範囲の特定に有効
- **バックアップ**
  - 参照系立ち上げのためのシステムのバックアップ
  - ワープロ端末のバックアップ
- **ネットワーク**
  - AD、アプリケーション、バックアップが同一にあると、バックアップ破壊、サーバー暗号化につながる
  - RDP ポートの変更の実施
  - 次期調達では、ネットワーク構成の分離を検討する
- **EDR、セキュリティ製品は万能ではない**
  - 攻撃者は、常に研究を行っている
  - 脆弱性対策、強いPW、標準ユーザー、ネットワーク分離、Syslog 取得等の多層防御の一つとして位置付ける

ありがとうございました。

※本日の講義でご紹介したリンク先は、アンケートに記載しております。
本研修ではリアルタイムでの質問はお受けしておりません。
ご質問のある方は、アンケートにご記入ください。

https://forms.gle/671iAgjuvHbh3Tpx5