ランサムウェア攻撃に関する情報提供（注意喚起含む）

Minaminihon Information Processing Center
株式会社南日本情報処理センター

ランサムウェア攻撃の概要

今回の医療機関でのランサムウェア感染について

データ復元と引き換えに金銭を要求する“ランサムウェア（身代金型）にウイルス感染。病院内の数十台のプリンタから英文の犯行声明が印刷される事態となった。

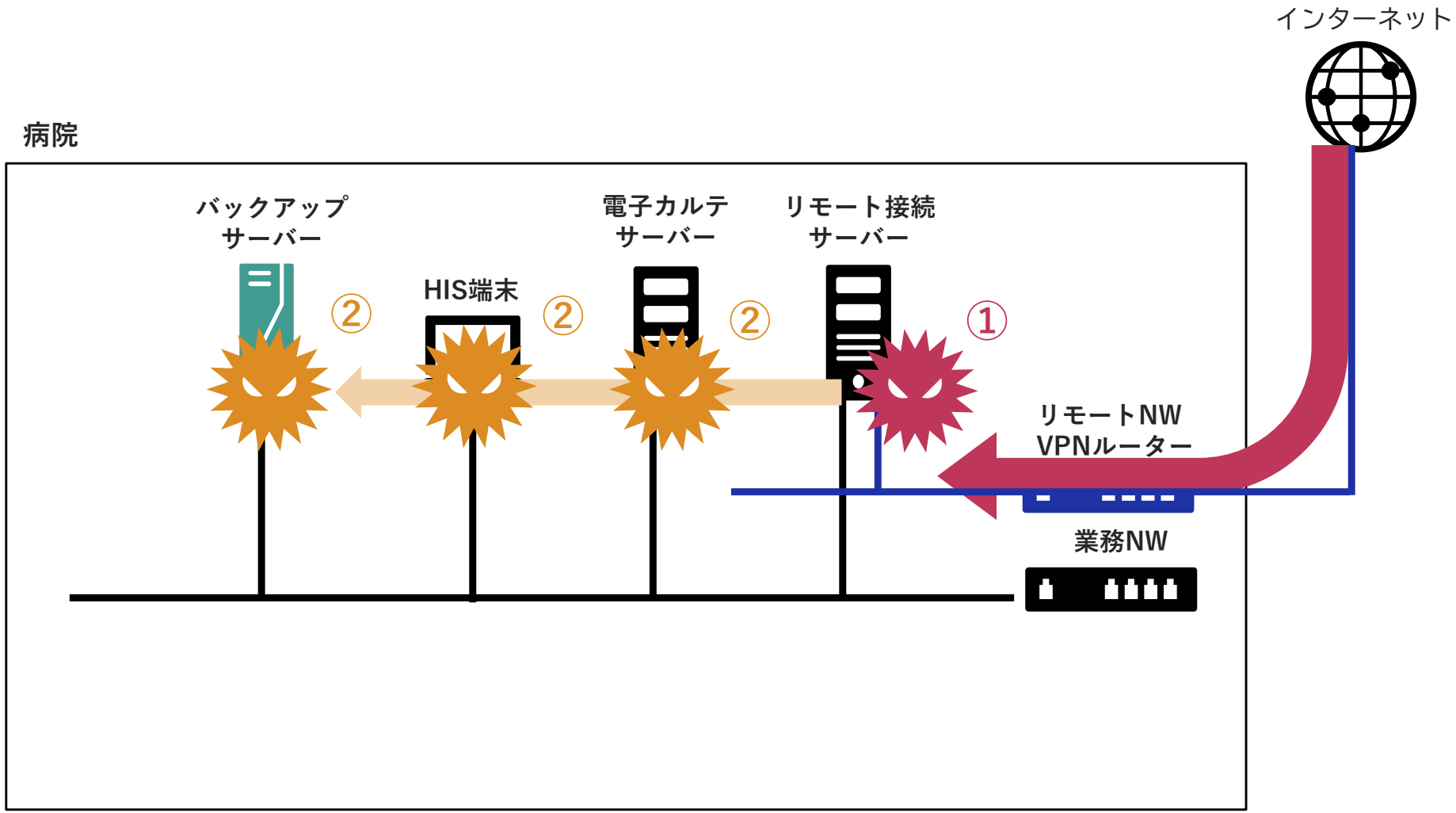
サーバのウイルス感染により8万5千人分の患者データにアクセスできず、電子カルテシステムだけでなく、医事会計システム等も利用できなくなり一部の診療科を除き、新規患者らの受入を中止することとなった。

原因は、リモート用ルータ機器（FortiGate）の脆弱性をつきシステムへ侵入。バックアップデータも感染したことからシステムの復旧ができない状況となり、診療再開に２カ月ほど時間を要するなど大きな事態へ発展した。

朝日新聞DIGITAl　記事参照
https://news.yahoo.co.jp/articles/d44998f74b07b750a74d067ca841b7d8862fbd11

ランサムウェア攻撃の概要

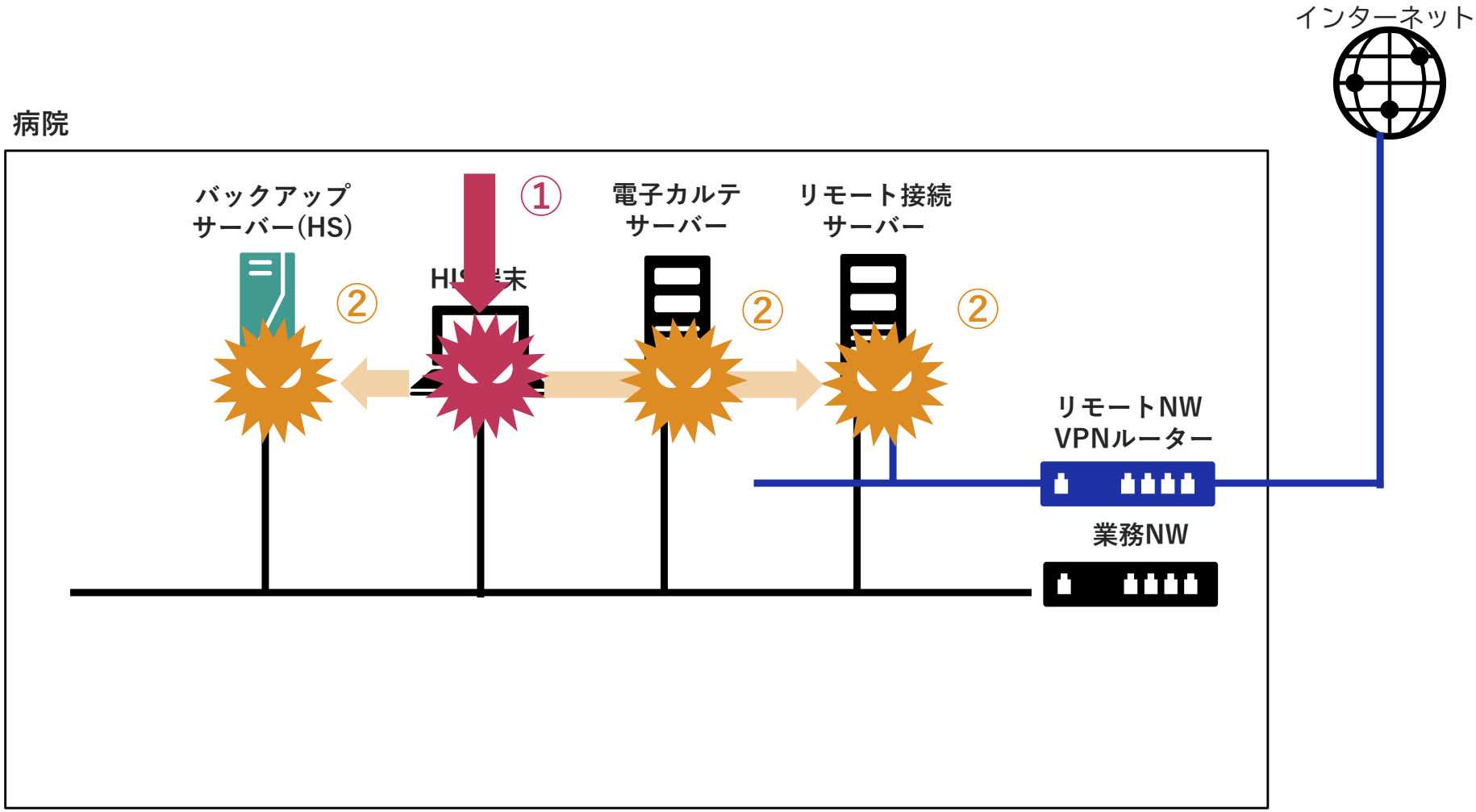
VPNルータから侵入、不正アクセスが原因
※ForiGateの脆弱性など



※日本電気株式会社
“22_ランサムウエア攻撃に関する情報提供（注意喚起）202112 .pdf”より、一部抜粋しております。

ランサムウェア攻撃の概要

HIS端末から侵入、ウイルス感染が原因
※USB利用等のルールを守らない



※日本電気株式会社
“22_ランサムウエア攻撃に関する情報提供（注意喚起）202112 .pdf”より、一部抜粋しております。

ランサムウェア攻撃の概要

マルウェアの感染、感染対策についてのポイント

■病院だけを標的にしているわけでは無く、脆弱な環境が標的

■IP-VPN（閉域網回線）以外の回線利用時は、VPNルータのファームウェア最新化をする必要あり

■HIS端末のウイルス対策ソフトの定義ファイルの最新化意は必須

■リモートデスクトップ接続の仕組みを悪用して感染するケースあり

■リモートサーバの接続履歴や、メモリ情報からログインID/PWを採取する手法あり

■バックアップをオフラインで2重化取得することが重要

サーバー攻撃対策とバックアップ規定が盛り込まれる見通し

⑩　診療録管理体制加算の見直し

第１　基本的な考え方

適切な診療記録の管理を推進する観点から、「医療情報システムの安全管理に関するガイドライン」を踏まえ、診療録管理体制加算について非常時に備えたサイバーセキュリティ対策の整備に係る要件を見直す。

第２　具体的な内容

非常時に備えたサイバーセキュリティ対策が講じられるよう、床数が 400 床以上の保険医療機関について、医療情報システム安責任者の配置及び院内研修の実施を診療録管理体制加算の要件にまた、医療情報システムのバックアップ体制の確保が望ましいこ件に加えるとともに、定例報告において、当該体制の確保状況に報告を求めることとする。

改　定　案	現　　行
【診療録管理体制加算】 ［施設基準］ 1　診療録管理体制加算１に関する施設基準 (1)　（略） (2) 中央病歴管理室が設置されており、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」に準拠した体制であること。 (3)～(9)　（略） (10) 許可病床数が400床以上の保険医療機関については、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」に基づき、専任の医療情報システム安全管理責任者を配置すること。また、当該責任者は、職員を対象として、少なくとも年１回程度、定期的に必要な情報セキュリティ	【診療録管理体制加算】 ［施設基準］ 1　診療録管理体制加算１に関する施設基準 (1)　（略） (2) 中央病歴管理室が設置されており、「医療情報システムの安全管理に関するガイドライン」（平成29年５月厚生労働省）（以下、「医療情報システムの安全管理に関するガイドライン」という。）に準拠した体制であること。 (3)～(9)　（略） （新設）

※中央社会保険医療協議会　第513回
「2　個別改訂項目（その１）について　中医協　総ー２４．１．２６」抜粋

マルウェアの感染、感染対策のご提案

その１＿VPNルータのファームウェア最新化

その２＿エンドポイント対策

その３＿バックアップの二重化

VPNルータのファームウェアの最新化

訪問先等からの外部接続環境および各システムのリモート保守で利用しているネットワークのVPNルータについては、ファームウェアの最新化を行い、脆弱性による攻撃に危険性を最小限にしてください。

詳細は、ネットワーク構築・保守業者へご相談いただくことを推奨いたします。

エンドポイント対策

■アンチウイルス対策ソフトの導入
■アンチウイルス対策ソフトの最新化

業務系ネットワーク、情報系ネットワークを問わず、ウイルス対策ソフトの導入および最新化を推奨いたします。

■承認されていないUSBメモリ等のデバイスを介したウイルス対策
感染リスクを減らすため、資産管理ソフト SecureSeed をご提案します。

・操作ログ取得、監視、ファイルトレース
・USBメモリ等のデバイス制御
・許可されていない機器の院内ネットワーク接続拒否

エンドポイント対策　SecureSeed

監視・アラート通知機能

【監視設定できる内容例】

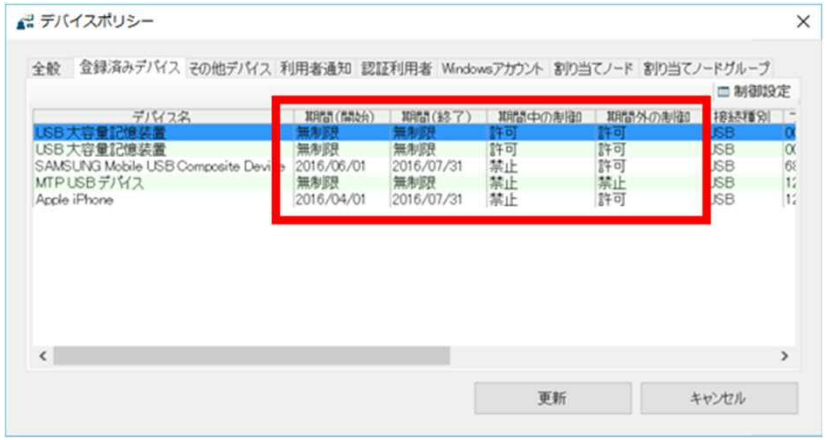
- 業務時間外のUSBメモリの利用
- 大量印刷
- 業務中のメールの起動
- 転職サイトなどのWEB閲覧
- 一定サイズ以上のメール送信
- アプリケーションのインストール・削除
- ファイルサーバの特定フォルダからのファイルの移動・コピー

設定した監視条件をもとに、セキュリティポリシーに反する操作を発見した場合に、管理者へメール、利用者へ通知します。

抑止効果も期待できます。

エンドポイント対策　SecureSeed

デバイス制御機能



USBメモリ、スマートフォン等のデバイスの利用を制限（利用可・読み込みのみ・利用禁止）にて私用デバイスによるウイルス持込を抑制することが可能です。

接続されたUSBデバイスを一覧から確認でき、利用者等の特定も可能です。

バックアップの二重化

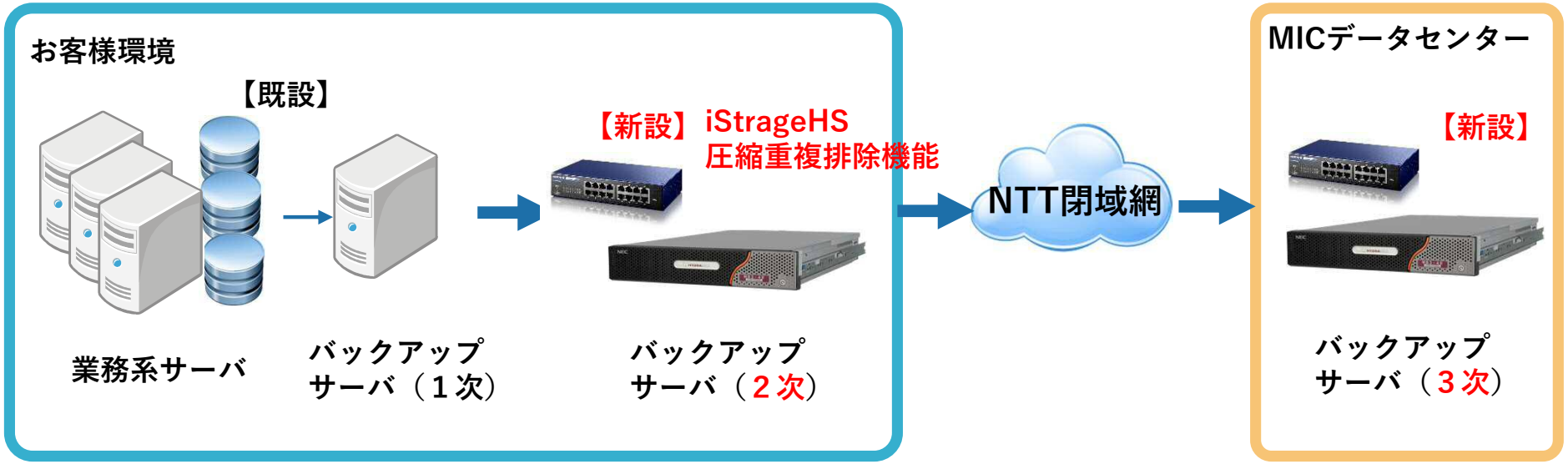
バックアップ二重化を行うことで、万が一、ランサムウェアに感染した場合に、ウイルス感染前のバックアップデータに復元し、システム復旧時間の短縮化し被害を最小限に抑える対策が図れます。

１．BCP対策を兼ね、遠隔地へバックアップを取得
　　NECサーバ　iStrageHSを利用

２．ローカル環境へバックアップを世代化して取得
　　ネットワーク通信制御による感染対策

バックアップの二重化　　遠隔地バックアップ

NEC製iStrageHSを新規導入し、効率的な遠隔地バックアップ

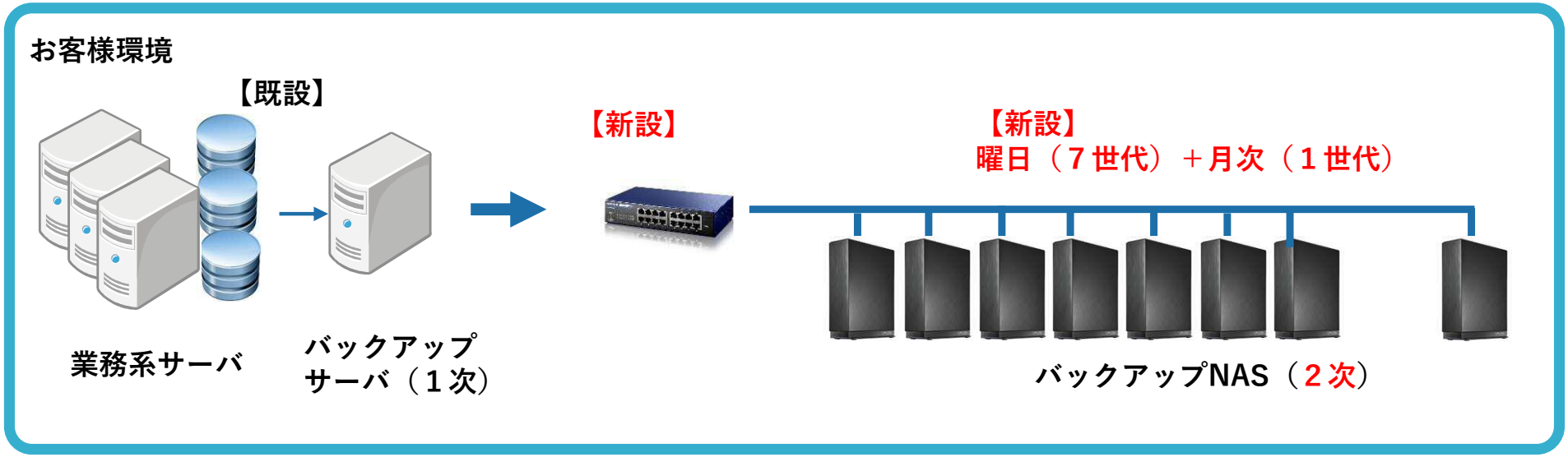


★既設バックアップサーバにてARCServeを利用してiStrageHSへバックアップ
★バックアップ時は圧縮重複排除機能にてバックアップ容量を最大１／２０に削減
★遠隔地のiStrageHSへ自動でレプリケーション
　※ブロック単位で差分コピーのためネットワーク負荷は軽減される
★お客様環境とMICデータセンターはフレッツ・VPNプライオ利用した閉域網で情報漏えいリスク減

ランサムウェア感染対策　その３

バックアップの二重化　　ローカル環境での世代管理

ルータとNASを新規導入し、感染リスクを抑え世代バックアップ



★バックアップサーバにて曜日毎にバックアップタスクを実行
★バックアップサーバのNICにIP設定し、該当バックアップの場合にのみ有効化
　通常は無効化しておき、曜日毎および月次のバックアップに指定したターゲットNASにのみ
　アクセスできるように設定・制限する
★NASはIP体系を分けることで、NAS間での通信をできないように論理的に遮断する

ICTで躍動、笑顔の創造

Smile Creation MIC

MIC 株式会社 南日本情報処理センター

医療福祉本部

〒891-0115 鹿児島市東開町4-104
TEL : 099(269)9720　FAX : 099(269)9719
URL : http://www.kk-mic.jp