2. 住基ネットにおける脅威の具体的イメージ

(1) ターゲットと入口
(2) 容易に想定できるターゲットへの経路

(1) ターゲットと入口

Targert - 1：事務処理システム（サーバー）・業務用クライアント上の個人情報
Targert - 2：既存住基システム（サーバー）上の個人情報
Targert - 3： CSサーバー（CSクライアント）上の本人確認情報
Targert - 4：都道府県サーバー・全国サーバー上の本人確認情報
Targert - 5：他の自治体のCSサーバー・庁内LAN上の本人確認情報・個人情報

入口- 1：インターネットからの不正な意図を持つアクセス
入口 - 2：庁内LAN(公共施設などのLAN）への不正規なクライアントの接続
ここには、ダイヤルアップルーターで接続された出先機関・公共施設などのLANへの不正規なクライアントの接続を含みます。
入口 - 3：ダイヤルアップルーターの偽装による庁内LANへの不正規なクライアントの接続
入口 - 4： CSサーバー／CSクライアントに直結するLAN配線への不正規なクライアントの接続

本報告では、個人情報が集中している各種のサーバーを主要なターゲットとして検討対象としますが、CSクライアントや事務処理用クライアント上にも、さまざまな個人情報が存在し、脅威にさらされていることに留意してください。

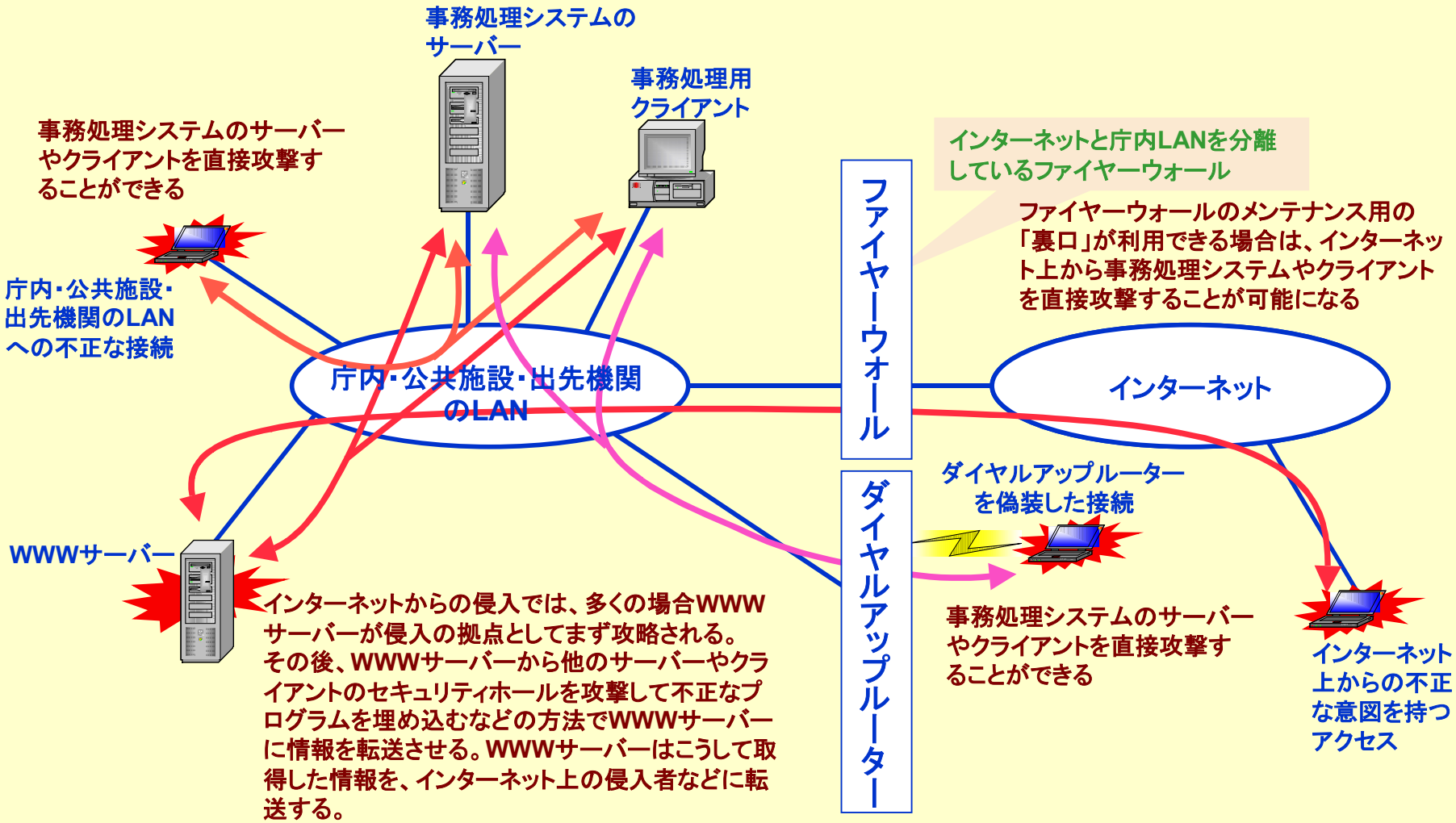
なお、Target-5については、長野県の実験範囲を大幅に超えるため、本レポートの対照とはしていません。Target-5については、本レポートの補遺として作成した「住基ネットを通じた他の自治体への不正侵入（住民票の写しの広域交付不正請求）についての検討」を参照ください。

また、「個人情報の書換」の結果発生するセキュリティ上の問題については、本レポートの範囲外とします。「書換」が可能であることは「参照」が可能であることを意味しており、本報告の検討範囲はこのような「参照」（漏洩）までとします。

(2) 容易に想定できるターゲットへの経路

拠点となるサーバーまたはクライアント

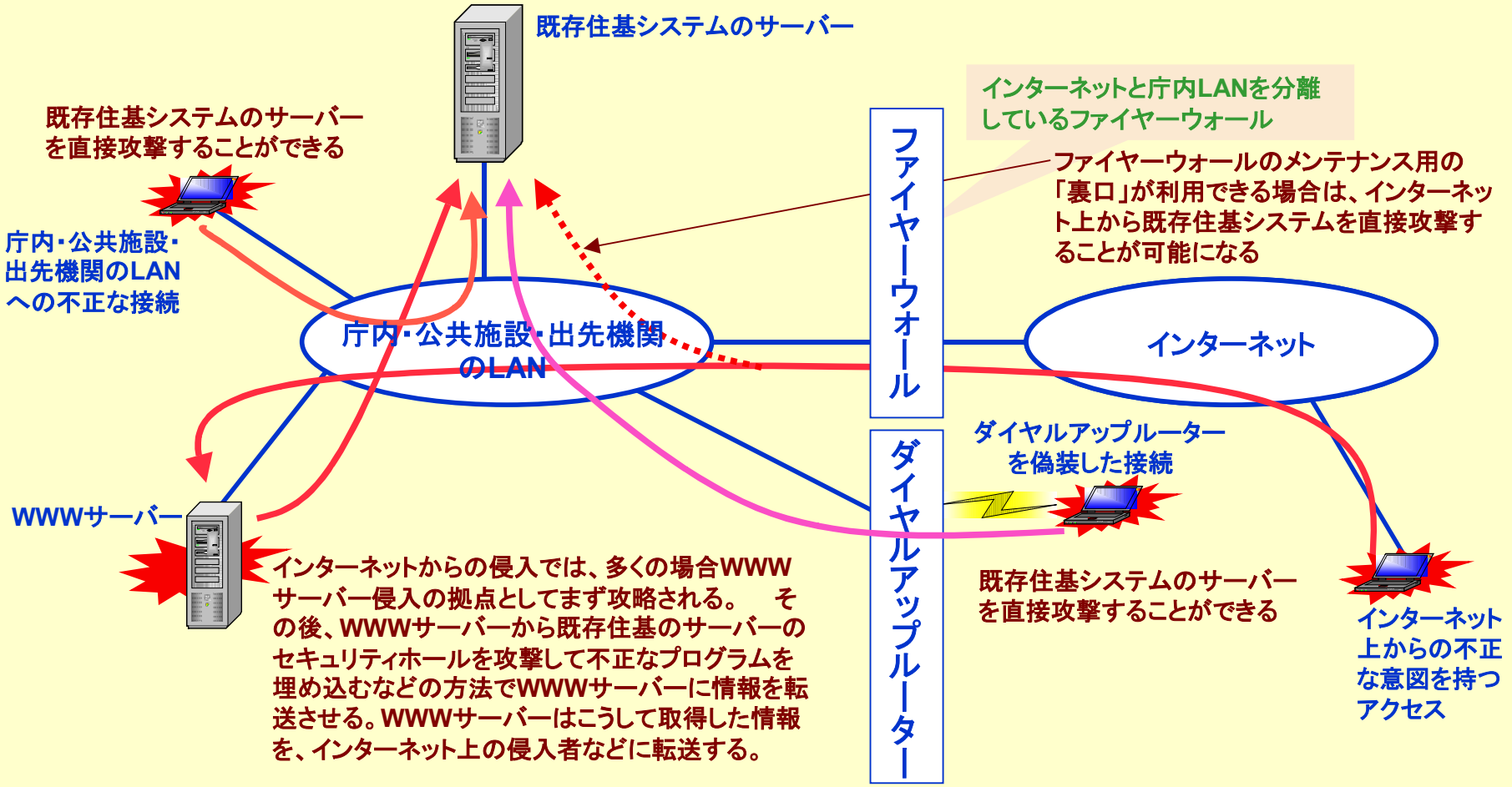
Targert - 1：事務処理システム（サーバー）・業務用クライアント上の個人情報



(2) 容易に想定できるターゲットへの経路

拠点となるサーバーまたはクライアント

Targert - 2：既存住基システム（サーバー）上の個人情報

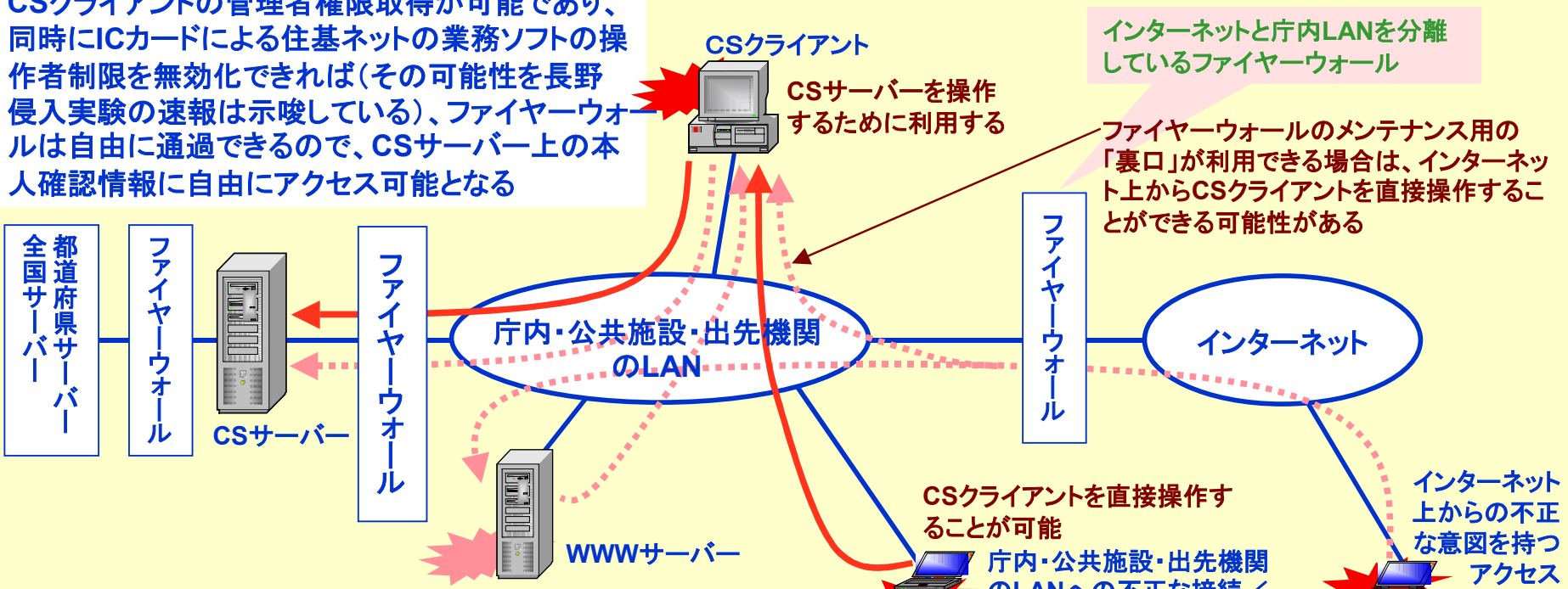


(2) 容易に想定できるターゲットへの経路

拠点となるサーバーまたはクライアント

Targert - 3: CSサーバー（CSクライアント）上の本人確認情報
（その１：庁内LAN側にCSクライアントがある場合）

CSクライアントの管理者権限取得が可能であり、同時にICカードによる住基ネットの業務ソフトの操作者制限を無効化できれば（その可能性を長野侵入実験の速報は示唆している）、ファイヤーウォールは自由に通過できるので、CSサーバー上の本人確認情報に自由にアクセス可能となる

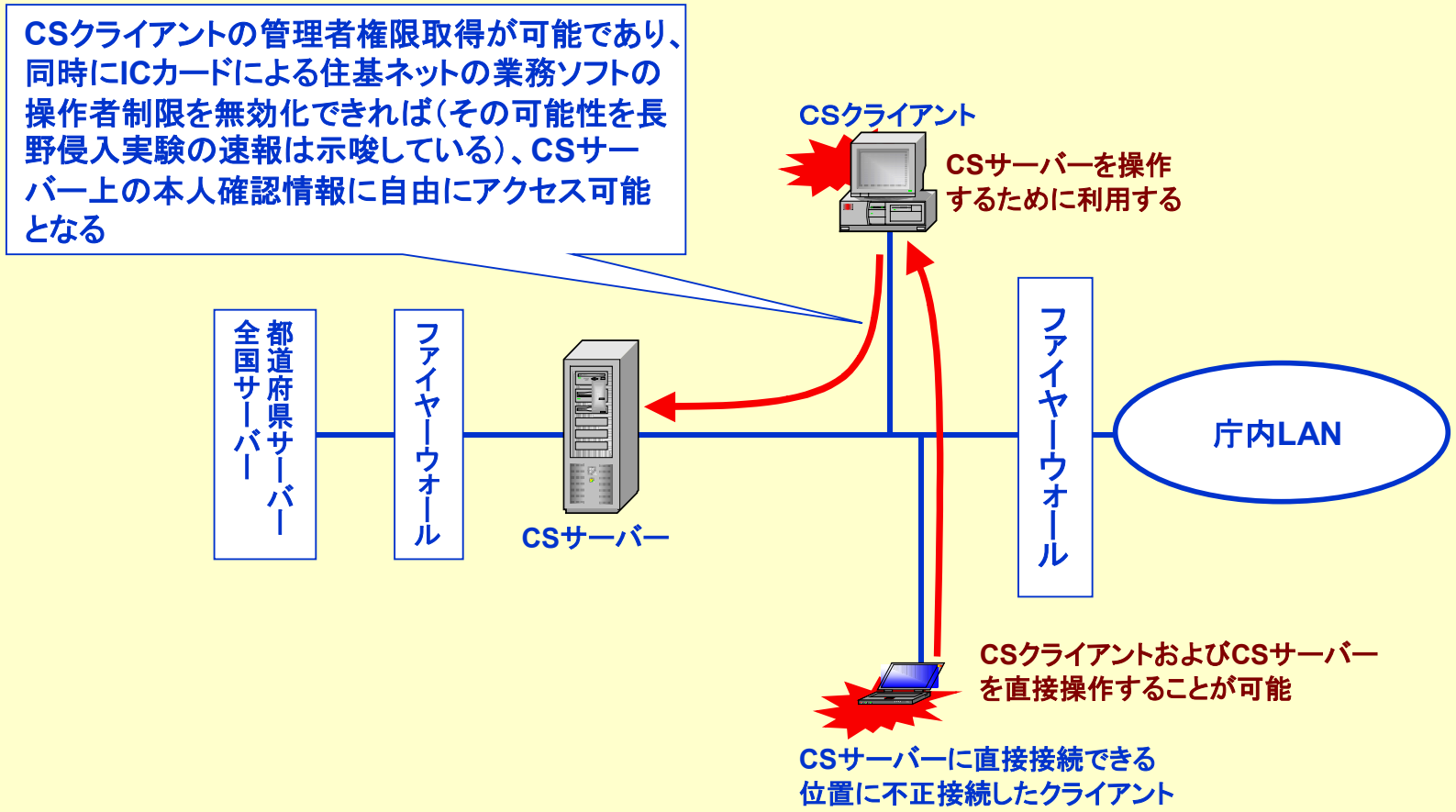


インターネットからWWWサーバーを拠点としてCSクライアントを攻撃する場合、ファイヤーウォールが有効であれば侵入操作はすべて間接的なものとなり、CSサーバー上の本人確認情報へのアクセスの困難度は高くなる。
しかし、CSクライアントがCSサーバーや都道府県サーバー・全国サーバーなどにアクセスした結果を受動的に監視し、その情報をインターネット上に転送することは比較的容易に実行できる。

(2) 容易に想定できるターゲットへの経路

拠点となるサーバーまたはクライアント

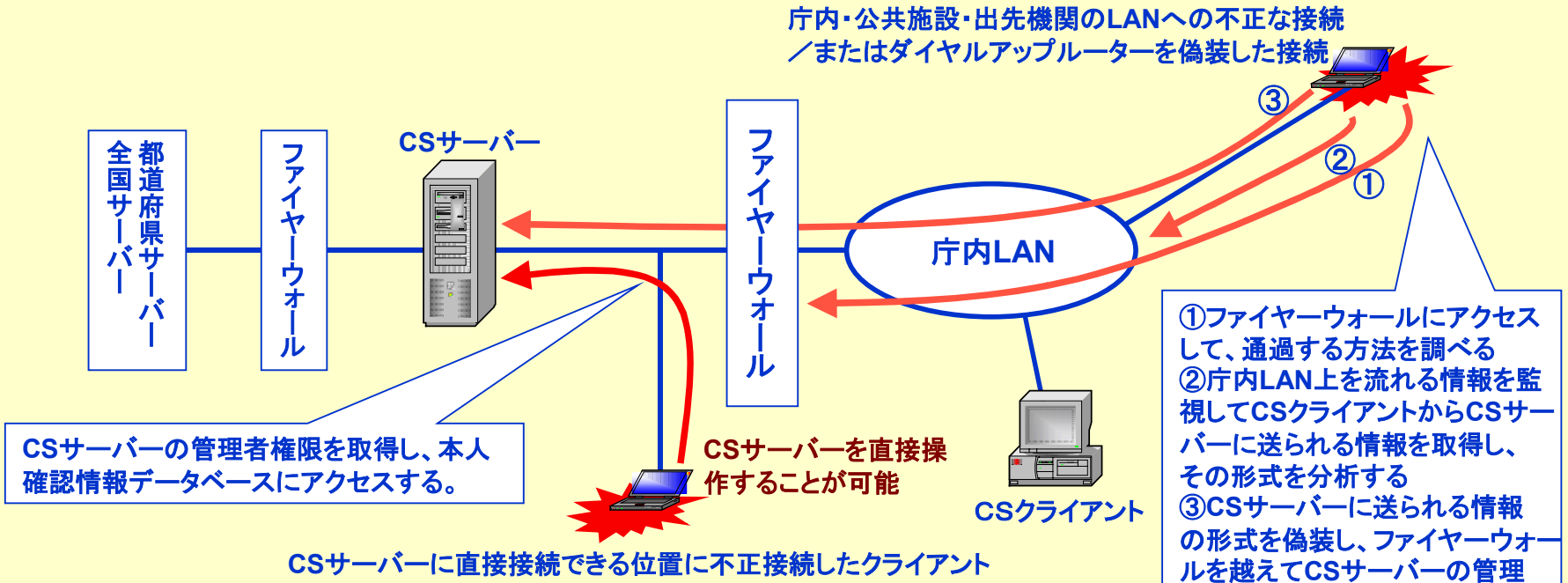
Targert - 3: CSサーバー（CSクライアント）上の本人確認情報
（その2：CSクライアントがCSサーバーに直結する場所にある場合）



(2) 容易に想定できるターゲットへの経路

拠点となるサーバーまたはクライアント

Targert - 3: CSサーバー（CSクライアント）上の本人確認情報
（その3：不正接続したクライアントから、CSサーバーを直接攻撃する場合）



直接アクセスおよび庁内LANからの間接的なアクセスのいずれの手法でも、本人確認情報データベースの内容を参照するためには、データベースの操作権限（アクセス権限）を取得する必要がある。長野県の実験では、この権限を取得したとは報告されていない。

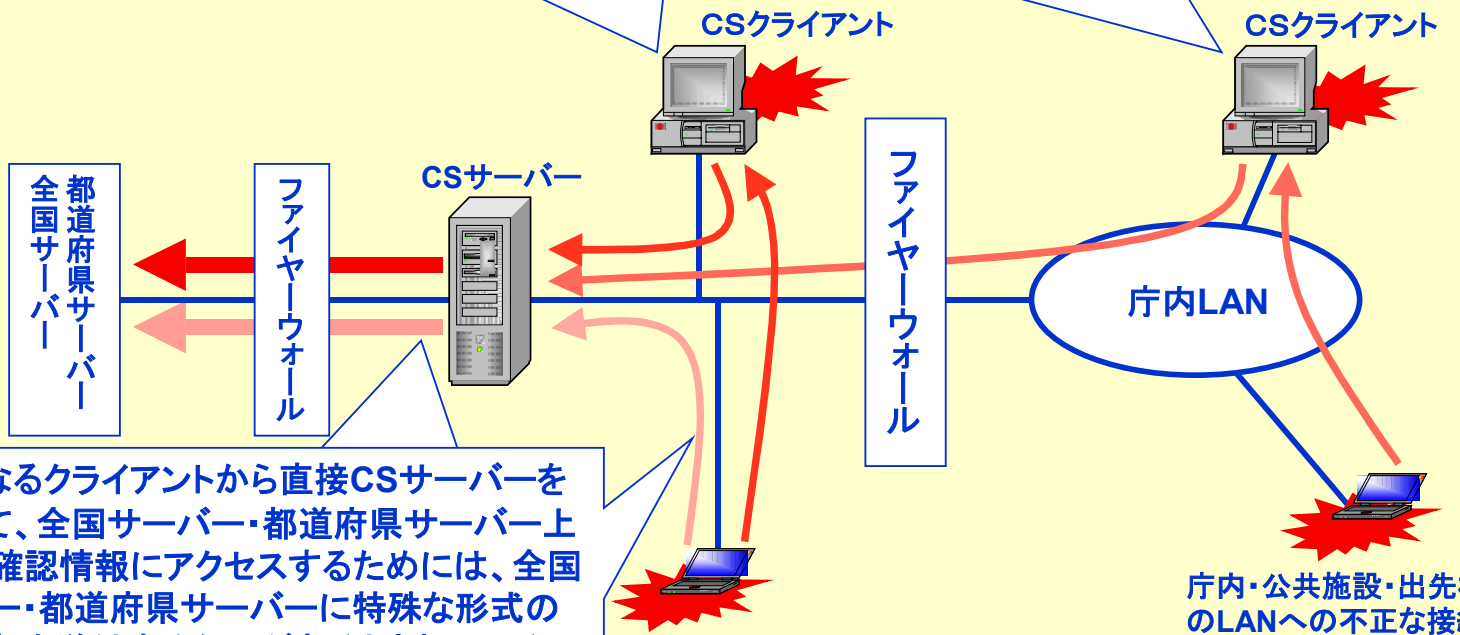
アクセス権限を取得できなくても、本人確認情報データベースのファイルを、一括してコピーすることは可能であり、ファイル単位で取得した後時間をかけて分析することによって本人確認情報を取得できる可能性がある。

(2) 容易に想定できるターゲットへの経路

拠点となるサーバーまたはクライアント

Targert - 4：都道府県サーバー・全国サーバー上の本人確認情報

CSクライアントの管理者権限取得が可能であり、同時にICカードによる住基ネットの業務ソフトの操作者制限を無効化できれば（その可能性を長野侵入実験の速報は示唆している）、CSサーバーを通じて都道府県サーバー・全国サーバー上の本人確認情報にアクセスすることは制限を受けない



拠点となるクライアントから直接CSサーバーを操作して、全国サーバー・都道府県サーバー上の本人確認情報にアクセスするためには、全国サーバー・都道府県サーバーに特殊な形式の命令情報を送付する必要があるとされている。このコマンドの形式は、CSサーバーの動作を監視し分析することで取得可能であると予想できる。