Vol.2012-CSEC-59 No.2
2012/12/14

ICHIGAN セキュリティ – 局面に応じたポリシーの切り替えを可能にするセキュリティアーキテクチャ

丸山宏[†1]　渡辺清[†2]　吉濱佐知子[†3]　浦本直彦[†4]　竹洞陽一郎[†5]

ICHIGAN は災害に強い自治体の参照アーキテクチャを作る，非営利のプロジェクトであり，自治体間でバックアップしあうカップリングと，災害局面に応じたモード切り替えに特徴を持つ．本稿では，局面によって自治体全体のセキュリティ・ポリシーを切り替える考え方を提案し，そのために必要なポリシーのテンプレートと，認証時の検証を遅らせる繰延認証の考え方を提示する．

ICHIGAN Security – A Security Architecture that Enables Situation-Based Policy Switching

HIROSHI MARUYAMA[†1]　KIYOSHI WATABE[†2]
SACHIKO YOSHIHAMA[†3]　NAOHIKO URAMOTO[†4] YOICHIRO TAKEHORA[†5]

Project ICHIGAN is a voluntary-based attempt to build a reference IT architecture for local governments that can withstand large-scale natural disasters. This architecture is unique in that 1) it has the concept of *mode* depending on the phases of the situation, and 2) the functionalities and services provided by the IT systems in the suffered area will be taken over by those of the "coupled" local government. These features pose specific challenges on the information security policy, especially because different policies need to be applied for the different modes. This paper describes two key elements to enable the policy; *policy templates* and *deferred authentication.*

1. はじめに

プロジェクト ICHIGAN[1]は災害に強い自治体の IT アーキテクチャを作る非営利のプロジェクトであり，ICHIGAN RA (Reference Architecture)とは，その参照アーキテクチャである．本稿では，ICHIGAN RA の一部である，ICHIGAN セキュリティ・アーキテクチャについて述べる．

我々は，ICHIGAN セキュリティ・チームとして，例えば次のようなシナリオを想定した．

202X 年，東南海・南海複合地震が発生，紀伊半島にある人口 16,000 人の自治体 A 町では津波の被害が甚大で自治体機能がほぼ麻痺状態となった．津波の発生から 3 時間後，A 町の自治体職員の B 氏のところへ，救援にあたっている自衛隊から連絡があり，被害が甚大な地区における住民リストの提出を求められた．カップリング（後述）先の自治体において被災者基本台帳システムが既に動いているのだが，担当部署の異なる B 氏にはアクセス権限がない．しかし，上司とはまったく連絡が取れず，町役場の指揮命令系統がどうなっているかも不明だ．B 氏はどうすればよいのだろうか？

ICHIGAN RA は，Concept of Operations (ConOps)[2]の概念に基づき，通常期，警戒期，緊急期，応急期など災害の局面に応じて，業務プロセスや IT システムの要件に異なる優先順位を与える[3]．これら局面に応じて優先順位が変更される要件の中には，機密性・可用性・完全性など，一般的に情報セキュリティ・ポリシーで規定されるべきものとして考えられるものも含まれる．例えば，緊急時には IC カードなどの本来の認証手段が使えないにもかかわらず，人命救助のためなどにシステムにアクセスする必要があるかもしれない．このため，セキュリティ・ポリシーも局面に応じて切り替える必要がある．

局面に応じたセキュリティ要件の切り替えを明文化したセキュリティ・アーキテクチャは，我々の知る限り他に類を見ない．このため，我々は本セキュリティ・アーキテクチャ策定にあたり，情報セキュリティに関する以下の３つの基本理念を常に意識するように心がけた．

1. ホリスティック・アプローチ： 情報セキュリティは弱い所から破られる．したがって，特定の観点で必要以上に強いセキュリティを求めないよう，配慮する．
2. 簡潔さ： 人が覚えられないポリシーは守ることができない．したがって，ポリシーは極限までに簡素化する．
3. 柔軟さ： 災害時には，あらかじめ想定することので

†1 情報・システム研究機構 統計数理研究所, Research Organization of Information and Systems, The Institute of Statistical Mathematics
†2 Microsoft Services
†3 IBM Research
†4 日本 IBM 東京基礎研究所, IBM Research – Tokyo
†5 Keynote Systems, Inc.

きない事態が多数発生すると考えられる．したがって，本アーキテクチャは，想定外の事態にもできるだけ柔軟な運用ができるよう，配慮する．

2. スコープ

自治体は，ISO27001[4]，総務省のガイドライン[5]などのベスト・プラクティスに基づいた情報セキュリティ・ポリシー体系をベースポリシーとして持っていなければならない．その上で，ICHIGAN RA 導入に基づく新たなスコープを定義する．ICHIGAN　RA が新たに導入する業務プロセス・IT システムには以下のものがある．

1. 被災時業務
   被災時業務には，被災者基本台帳登録業務や，安否確認など，災害前にあらかじめ計画できるものと，被災の種類や状況によって被災後初めて必要が判明する業務とがある．
2. 被災時 IT システム
   被災時 IT システムは，被災の状況に応じて，オフライン作業を余儀なくされるもの，携帯端末の利用を求めるもの，などがありうる．
3. カップリング．
   被災した自治体の業務を代行するため，業務プロセスまたは IT システムまたはその両方について，その主管あるいは運用を被災自治体から支援自治体へ移管すること．

ICHIGAN のセキュリティ・アーキテクチャが定義するスコープを図 1 に示す．

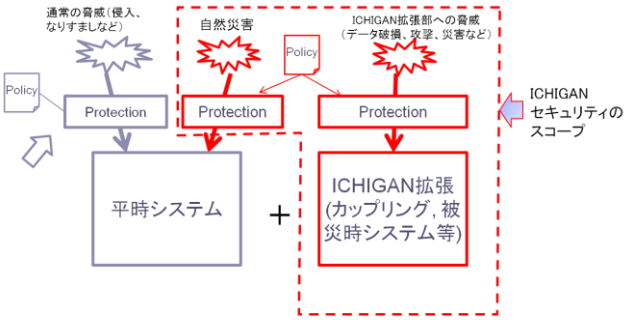

図 1　ICHIGAN セキュリティのスコープ
Figure 1　Scope of ICHIGAN Security

3. 災害における局面

ICHIGAN RA が定義する局面には，通常期，警戒期，緊急期，応急期，復旧期，復興期の 6 種類がある．平時とは，通常期か復興期である．被災時とは，警戒期，緊急期，応急期，復旧期のいずれかである．これらの局面は，ICHIGAN RA では以下のように定義される[3].

- **通常期**：災害発生前の局面．地方自治体は，平時の行政サービスを提供している．また，防災訓練・演習を実施している．
- **警戒期**：災害の発生が予見され，災害に対する警戒を行う局面．自治体首長による警戒体制の確立の宣言により，本局面に移行する．平時システムのカップリング先への切り替えや，被災時システムの起動を行う．
- **緊急期**：自治体首長による住民への避難勧告が発令されることで本局面に移行する．避難所の設置や要員の配置や，関係組織への支援依頼などが行われる．被害発生時には，警察・消防・自衛隊などによる捜索・救助などが実施される．ネットワーク輻輳／電源喪失などが原因で，被災自治体に設置された平時システムが利用できない場面を想定する．
- **応急期**：緊急期を脱し，避難所での行政サービスが本格的に開始されることで本局面に移行する．避難者安否確認，避難物資の調達と配給などのサービスが，被災者に対して提供される．復旧した平時システムで重要な平時行政サービスを縮退状態で継続する，被災時システムを立ち上げネットワーク品質が悪い避難所においてタブレットやスマートフォンなどで被災時業務アプリケーションとデータを利用する，などの場面を想定する．
- **復旧期**：自治体首長による警戒体制の解散宣言により，本局面に移行する．り災・被災証明の発行，義捐金・給付金の配布，被災者の自宅への帰還，仮設住宅への移動の開始，復旧事業に必要な行政サービスに対応する自治体システムの立ち上げ，などの場面を想定する．
- **復興期**：避難所の閉鎖，災害からの復興事業の開始などのイベントにより本局面に移行する．平時の行政サービスは通常期と同等に提供されると想定する．

典型的な局面の遷移を図 2 に示す．この遷移は標準的な順序関係だけを規定している．実際には，警戒期から通常期に戻るなど，途中をスキップした遷移がありうる．

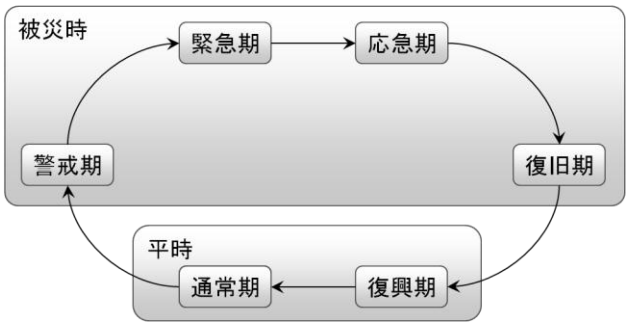

図 1　ICHIGAN RA における局面
Figure 1　Phases Defined in ICHIGAN RA.

本稿では，簡単のため，通常期，緊急期，応急期の 3 局面のポリシーについてのみ考える．

4. ポリシーの切り替え

一般に，情報セキュリティ・ポリシーは，情報セキュリテ

ィ方針，情報セキュリティ規定，各プロセスやシステム毎のガイドラインなど複数の文書から構成されている．これらの文書の特定の組み合わせをポリシー・セットと呼ぶことにする．自治体単位で，ある一時点で有効なポリシー・セットは唯一つである．以下に，ICHIGAN RA が推奨するポリシーのテンプレートの要点を示す．各自治体は，このテンプレートを用いて，それぞれの実態に即したポリシー・セットの見直しを行う．

4.1 情報資産の分類

ICHIGAN RA では，被災時に被災者台帳管理などの被災時システムが稼働することを想定している．これらのシステムは，機密性・完全性よりも可用性を重視する運用が行われることになるだろう．たとえば，後に述べる繰延認証によるユーザにアクセスを許すなどの状況がありうる．しかし，そのことによって自治体が本来持っている情報の機密性・完全性ができるだけ損なわれないようにしなければならない．

このため，情報資産に関し，自治体が持っている本来の区分に加えて以下の分類を行う

- 秘匿性重視（Confidentiality Sensitive）
  秘匿性が高く，かつ被災時に緊急にアクセスする必要が無いもの．たとえば，住民のデータ項目のうち，収入に関するもの，など．秘匿性重視の情報は，被災時システムで扱ってはならない．一方，通常個人情報として保護すべきもの（氏名・住所など）であっても，被災時システムで必要とされる情報資産については，秘匿性重視としないものとする．
- 完全性重視（Integrity Sensitive）
  被災時システムで入力された情報は，現場の混乱や緩い認証などの原因によって，完全性が充分でないかもしれない．従って，これらの情報に基いて被災時システムから平時システムへの更新が行われると，平時システムの完全性が損なわれる可能性がある．従って，特に完全性への要求が高い情報資産に関しては，被災時システムから平時システムへの更新を許さない．
  例： 監査証跡．また，住民のデータ項目のうち，氏名や生年月日などの基本項目

4.2 通常期ポリシー

通常期には，基本的に自治体が本来持っているポリシーを適用する．加えて，警戒期あるいは緊急期への切り替えのための手続きを定義しなければならない．これは通常，自治体の首長の宣言により行われる．ただし，自治体の意思決定機能が事実上失われている場合には，自動的に緊急期へ切り替えられるよう，ポリシー上に明文化して置かなければならない

また，通常時ポリシーの中には，ポリシーの切り替えを含む，ICHIGAN アーキテクチャに基づくシステムの訓練・テストを可能にするための条項を盛り込んで置く必要がある．

4.3 緊急期ポリシー

緊急期とは，情報の可用性が人の生死を左右するような局面である．このため，機密性・完全性よりも可用性を特に重視しなければならない．また，現場の判断をできるだけ尊重する．災害発生から 72 時間が経過すると生存率が急激に低下することから，緊急期ポリシーの適用は災害発生から 72 時間の適用を目安とする．

このポリシーは，原則として被災時システムに対してのみ適用する．ただし，被災時システムが立ち上がっていず，かつ緊急性がある場合には，災害対策本部の判断により，平時システムにも一時的に適用してもよい．

緊急時には，IC カードを紛失していたり，ネットワークが切断されてディレクトリにアクセスできなかったりすることが考えられる．それにも関わらず，「誰がどこにいるか」などのクリティカルな情報にアクセスする必要がある．このため，我々が繰延認証と呼ぶ認証手続きを許す．

4.3.1 繰延認証 (Deferred Authentication)

繰延認証とは，アクセス時にユーザーの身元（ID）のクレーム情報（「私は XX である，その証明は YY である」）は収集するが，その検証はアクセス時には行わず，事後に検証する方法を指す．例えば，ユーザーID 及びパスワードの入力を求めるが，その場ではディレクトリに対して値の検証を行わない．あるいは，ユーザー名と共に，ユーザーのバイオメトリクス情報（指紋・顔写真等）を保存する．ディレクトリが利用可能になった時点で，それらの検証を行う．

クレーム情報の収集は，現場の判断で柔軟に行なって良い．例えば，「12 月 14 日 11:35 自衛隊〇〇１尉の依頼により，丸山が管理者権限でログイン，確認吉濱．」などの記録を残すことも，クレーム情報の収集と考えられる．あるいは，端末室に緊急時に最低 72 時間稼働する監視カメラを設置するのでも構わない．

繰延認証が行われた場合，緊急期が終わり次第，可及的速やかにすべての繰延認証の検証を行わなければならない．また，この検証において，不正なアクセスが発見された場合には，セキュリティ事故として扱わなければならない．また，不正なユーザーID の下で行われたすべてのデータベース更新作業について，取り消しが行えるよう，監査証跡を残さなければならない．

繰延認証は本来の意味の認証ではない．したがって，繰延認証が行われた場合，システムの機密性・完全性が損なわれるリスクは高くなることは常に意識しなければならない．

4.4 応急期ポリシー

災害が発生して後，人命救助等の緊急の作業が一段落する

と，自治体はある程度の組織的な機能を回復し，応急期に入る．応急期には，被災者基本台帳登録業務や，安否確認に加えて，避難所の管理業務など，被災時業務が自治体 IT システムの主な利用目的となる．

4.4.1 被災時システムの開発と受け入れ

被災時のアプリケーションは，被災者基本台帳登録業務など事前に開発・テストしておける性質のものもあれば，昨年の原子力発電所の事故に伴う放射線量測定・開示のシステムのように事前に想定できずに，災害が発生してから開発しなければならないものもありうる．これらのアプリケーションは，通常とは異なる非機能要件を持つ．すなわち，バグや性能，使いやすさ，あるいはセキュリティをある程度犠牲にしても，ただちに運用に入る必要がある．また，これらのアプリケーションの一部は，通常の購買手続きに従って発注されるのではなく，ボランティアによって開発されるかもしれない．このようなアプリケーションに対しては，平時におけるセキュリティが求める変更管理プロセスを適用するのは無理がある．

このため，被災時システムの開発・受け入れに関しては，通常の変更管理プロセスを大幅に簡略化してもよいものとする．例えば，避難所等で使われるアプリケーション等については，その緊急度に応じて，通常行われる設計段階でのレビューや試験をスキップしても構わない．ただし，これらのアプリケーションについても，本アーキテクチャが規定する，応急期の他の要件（以下の述べるインフラ要件等）を満たす必要がある．

4.4.2 インフラ要件

避難所等においては，電力や通信などのインフラが制限されることもあるため，セキュリティ確保が難しい PDA 等でオフライン作業を行わなければならないことがある．また，支援物資として提供された PC には，本来のセキュリティ・ポリシーでは許されない，古いバージョンのオペレーティングシステムが動いているかもしれないし，最新のアンチウィルスが動いていなかもしれない．また，暗号化されていない WiFi など，保護されない通信路を使わなければならないかもしれない．

これらの状況に鑑み，応急時のインフラに対してもセキュリティ要件を軽減する．ただし，平時システムのセキュリティレベルが下がってはならない．このため，被災時システムと平時システムとの間に適切な分離機能（ネットワークでのファイヤーウォールなど）を入れることを要求する．

4.4.3 認証

被災時業務においては，他自治体の職員，自衛隊，ボランティアなど，被災自治体の職員でない多くの関係者がシステムを利用することになる．これらの利用者に対して，本来の自治体システムが持っている ID 管理方法に基いて ID を発行するのは現実的でない．

このため，応急時には，認証における緩いフェデレーションを許す．例えば，関連する自治体における認証，国の政府機関における認証，企業や大学等における認証などを利用する．これにより，支援自治体や自衛隊等の職員が，個別の登録作業をすることなく，被災時システムにアクセスできるようになる．

4.4.4 被災時システムの情報資産

秘匿性重視の情報資産は，被災時システムで格納・処理してはならない．また，被災時システムで処理された情報は，平時システムへのライトバック時に，適切な完全性検証プロセスを経なければならない

4.5 局面の通知

本アーキテクチャを運用する上で，最も大切なことは，現在の局面に関して，すべてのステークホルダが共通の理解を持っていることである．このため，自治体は，現在の局面が何であるかを，明確に曖昧さなく各ステークホルダに伝える仕組みを持っていなければならない．特に，被災時システムの画面上には常に現在局面を表示しておくなど，関連する職員等が常に現在適用されているポリシー・セットが何であるかを意識できるようにするべきである．

また，悪意により，あるいは事故により間違って局面切り替えが行われないように講じる対策も必要である．

5. IT プラットフォーム上の考慮点

上記のポリシーを実現するためには，IT プラットフォームに特有の考慮点がある．ICHIGAN RA では，アプリケーション・アーキテクチャ(AA)，データ・アーキテクチャ(DA)を制定中であり，これらのセキュリティ考慮点は，これらに文書に組み込まれる予定である．

5.1 認証の仕組み

緊急期・応急期には，それぞれ繰延認証やフェデレーションを行う必要がある．このため，被災時システムにおいては，プラグイン可能な認証の仕組みを持つことが望ましい．

5.2 監査証跡と ID の伝搬

緊急期や応急期には，認証のセキュリティレベルが低下することから，不正ユーザーによる機密情報の漏洩や情報の改ざんが行われることも否定出来ない．ICHIGAN RA では，このような事故の調査を事後に簡単に行えるようにすることで，被害の分析や，攻撃の抑止を図る．なお，監査証跡は，管理者によっても容易に削除できないようにするべきである．

ICHIGAN RA では，各システムが保持するべき監査証跡の項目とフォーマットを規定する．特に，データベースへのアクセスについての監査証跡が重要であり，このためにはアプリケーションが，エンドユーザーの身元情報をデータベースまで伝播させる必要がある．アプリケーション・アーキテクチャは，このような機能を持つミドルウェアを指定すべきである．

5.3 局面状態の保持

ICHIGAN RA では，セキュリティに関する多くのコンポーネントが，現在の局面状態を参照することになる．このため，現在の局面状態を複数のシステムに間違いなく伝えられるようにする仕組みが必要である．また，この局面状態を攻撃者が勝手に変更できると，大きな脆弱性となる．このため，この局面状態保持・通知機構は，改ざんに対して極めて堅固でなければならない．

6. ICHIGAN RA の適用

ICHIGAN RA は，災害の局面に応じて IT システムの非機能要件が変わる可能性があるということを前提にしている．このことは，セキュリティの観点からは，平時に定められたセキュリティ・レベルが，緊急期・応急期には変化することを意味している．このため新たに生じるセキュリティ・リスクに対して，自治体は適切に対処しなければならない．

このため，ICHIGAN RA を導入しようとする自治体の CISO は，上述の ICHIGAN セキュリティ・ポリシーをテンプレートとして，現行の情報セキュリティ・ポリシーの見直しを以下のステップで行うことを ICHIGAN セキュリティでは推奨している．

0. スコープの定義
1. 脅威モデルの定義
2. セキュリティ目標の設定
3. 局面ごとのポリシー・セットの定義
4. IT アーキテクチャへの要件定義
5. 運用ガイドラインの定義

特に，脅威モデルの定義とそれに基づくセキュリティ目標の設定は，自治体が災害における IT のシステムのあり方をどのように考えるか，ということに深く関わっていて，多くのステークホルダとの調整を通して，適切なリスク管理を行う必要があると考える．

7. おわりに

多くのセキュリティ・ポリシーには，「非常時にはこの限りではない」とか「非常時には情報セキュリティ責任者の判断により要件を緩和することがある」のような条項が設けられていて，それが非常時の柔軟な運用の根拠となっている．ただし，自治体における広域災害のような場合に，ガイドラインなくそれぞれの現場の判断で異なるやり方を用いるのは危険である．我々は，ポリシー・セットの切り替えというコンセプトにより，災害時にも共通したセキュリティ・レベルを確保するという考え方を提唱し，ICHIGAN セキュリティ・アーキテクチャという形で文書化した[6]．

ICHIGAN RA はリファレンス・アーキテクチャであり，このアーキテクチャを参照して各自治体が独自の IT システムを構築・運用していくことを狙っている．今のところ ICHIGAN RA はまだ作業中であるが，今後このアーキテクチャを採用する自治体が現れてくるものと期待している．ICHIGAN セキュリティは，局面に応じてポリシーを一括して切り替える，という新しい試みであり，現実に適用するには多くの議論が必要になることだろう．

参考文献

1) Project ICHIGAN, http://www.project-ichigan.jp/.
2) IEEE 1362-1998 , IEEE Guide for Information Technology – System Definition – Concept of Operations (ConOps) Document, 1998.
3) Project ICHIGAN, ICHIGAN Concept of Operations, 2012 (現時点で未公開).
4) ISO27001, Information Security Management System, ISO27001.
5) 総務省，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, http://www.soumu.go.jp/denshijiti/jyouhou_policy/index.html.
6) Project ICHIGAN セキュリティ・チーム, ICHIGAN セキュリティ・アーキテクチャ, 2012.