米国HIPAA／HITECH総括規則の動向

（日本語訳）

2013年12月

日本クラウドセキュリティアライアンス
健康医療情報管理ユーザーワーキンググループ
Health Information Management User WG
Cloud Security Alliance Japan Chapter

日本語訳 の提供について

- 「HIPAA／HITECH総括規則の動向」は、Cloud Security Alliance Health Information Management Working Groupよりリリースされている「CSA Cloud Bytes: An Overview of the HIPAA Omnibus Rule」（2013年6月）の日本語訳です。このドキュメントは、健康医療分野のセキュリティに関心のあるクラウドユーザーの教育・啓発を目的として、原文をそのまま翻訳したものであり、日本独自の法令や基準に関する記述は含まれておりません。
  なお、日本クラウドセキュリティアライアンスに関する情報は、以下のURLより参照可能ですので、ご覧下さい。
  http://www.cloudsecurityalliance.jp/
- このドキュメントは、以下の日本クラウドセキュリティアライアンスの有志により作成されています。
  - 日本クラウドセキュリティアライアンス・健康医療情報管理ユーザーワーキンググループ
    - リーダー：笹原 英司 （特定非営利活動法人ヘルスケアクラウド研究会 医薬学博士）
    - 阿倍 克英 （特定非営利活動法人ヘルスケアクラウド研究会）
    - 里中 慧 （特定非営利活動法人ヘルスケアクラウド研究会）

米国HIPAA／HITECH総括規則の動向

米国HIPAA／HITECH総括的規則の沿革

年月日	内容
2009年8月24日	HITECH法（Health Information Technology for Economic and Clinical Health Act of 2009）暫定的最終規則（IFR：Interim Final Rule）（データ漏えい）
2009年10月7日	遺伝子情報差別禁止法（GINA：Genetic Information Nondiscrimination Act of 2008）規則制定案告示（NPRM）（GINA規則）
2009年10月30日	HITECH法 暫定的最終規則（IFR）（執行）
2010年7月14日	HITECH法　規則制定案告示（NPRM：Notice of Proposed Rulemaking）（HITECH規則）
2013年1月25日	HIPAA総括規則（データ漏えい、執行、HITECH規則、GINA規則）公表
2013年3月26日	HIPAA総括規則（データ漏えい、執行、HITECH規則、GINA規則）施行
2013年9月23日（予定）	適用対象主体および事業提携者（BA：Business Associates）の遵守義務開始

米国HIPAA／HITECH総括規則の動向

米国HIPAA／HITECH総括的規則のスコープ

- 漏えい発生時の通知基準の改正
- 電子健康記録（EHR）に含まれる情報に対する患者のアクセス
- 事業提携者（BA：Business Associates）および下請け事業者に対する規制
- 許諾のないマーケティングにおける保護対象保健情報（PHI：Protected Health Information）の利用／開示の制限
- 許諾のない保護対象保健情報（PHI）の販売の禁止
- データの研究利用　- 複合的、より一般的な許諾
- 患者が保険者とのデータ共有を制限する権利
- プライバシーの取り扱いの通知を修正／再配布するための要件
- 契約査定のための遺伝子情報利用に対する制限の包含
- 民事制裁金（CMP：Civil Money Penalty）の執行／賦課および代理人行為の民事制裁金負債における保健社会福祉省（HHS：Department of Health and Human Services）長官の役割の明確化

米国HIPAA／HITECH総括規則の動向

米国HIPAA／HITECH総括的規則の対象外領域

- 各個人に対する情報開示の記録（検討中）
- HIPAA違反により侵害を受けた個人に対する、民事制裁金もしくは回収した和解金の分配方法（規則の提案はなし）
- 公民権局（Office for Civil Rights）が、後日、HIPAA対象外の個人健康記録（PHR）に関するプライバシー保護の報告および最小限必要な基準の導入に関するガイドラインを予定
- HITECHは、心理療法記録（Psychotherapy Notes）の定義に関する研究を委託（研究の終了時期は未定）

米国HIPAA／HITECH総括規則の動向

米国HIPAA／HITECH総括的規則と事業提携者（BA）（1）

- 事業提携者（BA：Business Associates）＝適用主体に代わって、保護対象保健情報（PHI：Protected Health Information）を生成、収集、維持、交換する者
  - 事業提携者（BA）に代わって保護対象保健情報（PHI）を生成、収集、維持、交換する、事業提携者（BA）の下請け事業者も該当する
  - 事業提携者（BA）としての位置づけは、契約上の相手関係ではなく、役割や責任に基づく
- 事業提携者（BA）に該当する例
  - 患者安全組織
  - 保健情報連携組織、電子処方箋ゲートウェア、適用主体の個人健康記録（PHR）ベンダー（全てのPHRではない）
  - 日常的に、保護対象保健情報情報（PHI）へのアクセスを必要とするデータ交換プロバイダー
- 事業提携者（BA）に該当しない例
  - 単にデジタル管路を提供する、データ交換サービス事業者は該当しない
  - ただし、実際に閲覧する意図がなくても、保護対象保健情報情報（PHI）を保存する事業者は該当する（例．クラウドモデルの電子健康記録（EHR））

米国HIPAA／HITECH総括規則の動向

米国HIPAA／HITECH総括的規則と事業提携者（BA）（2）

- 事業提携者（BA）と下請け事業者の関係
  - 適用主体と事業提携者（BA）との間の契約：事業提携者（BA）の下請け事業者は、事業提携契約書（BAA：Business Associate Agreement）の要件を満たすことが必要
  - 下請け事業者の下請けも、事業提携者（BA）に該当する
  - 結果として、事業提携者（BA）に適用されるHIPAA／HITECHの義務は、下請け事業者にも直接適用される
- HITECHの影響
  - HITECH施行前：事業提携者（BA）は、事業提携契約書（BAA）の遵守が求められる
  - HITECH施行後：事業提携者（BA）および下請け事業者は直接HIPAAの遵守が求められる

米国HIPAA／HITECH総括規則の動向

米国HIPAA／HITECH総括的規則と事業提携者（BA）（3）

- 保護対象保健情報（PHI）の利用について
  - 事業提携者（BA）は、事業提携契約書（BAA）で認められた場合もしくは法令で要求された場合のみ、保護対象保健情報（PHI）を利用／開示できる
  - 事業提携者（BA）は、プライバシー規則に違反する方法で、保護対象保健情報（PHI）を利用／開示することはできない
  - 下請け事業者は、適用主体と事業提携者（BA）間の契約書に基づき、制限することがある（下請け契約書で通知することが必要）
  - 必要最低限の規則に準拠していない場合、事業提携者（BA）は、利用／開示することが許されない
  - 下請事業者に法令違反があることを知りながら、漏えい対策など、妥当な処置を講じない場合もしくは処置が不十分で契約関係を終了した場合、事業提携者（BA）は、遵守していないとみなされることがある

米国HIPAA／HITECH総括規則の動向

米国HIPAA／HITECH総括的規則と事業提携者（BA）（4）

- 規制当局の権限について
  - 保健社会福祉省（HHS）長官は、事業提携者（BA）（下請け事業者含む）に対する不服申し立てを受けて調査し、不備な点や法令違反に対して、必要な処置を行う権限を有する
  - 事業提携者（BA）（下請け事業者含む）は記録を保持して、法令遵守報告書を当局に提出すると共に、不備な点の調査やコンプライアンスレビューに協力し、当局に対して情報へのアクセスを提供しなければならない
  - 事業提携者（BA）（下請け事業者含む）は、不服を申し立てた人に対し、威圧したり差別したりすることが禁止されており、規制当局に協力して、違法行為に反対しなければならない
  - 事業提携者（BA）（下請け事業者含む）は、HIPAA違反に対する民事制裁金を科せられることがある
  - 事業提携者（BA）（下請け事業者含む）は、適用主体（CE）／事業提携者（BA）の契約下で責任を負う

米国HIPAA／HITECH総括規則の動向

米国HIPAA／HITECH総括的規則と個人の権利（1）

- HITECH法により、各個人は、保護対象保健情報（PHI）の漏えいの通知を受ける権利が制定された
  - 漏えい＝「権限のない保護対象保健情報（PHI）の購入、アクセス、利用、開示で、情報のセキュリティやプライバシーを損なう・・・」
  - 権限のないデータ利用がない限り、適用主体（CE）／事業提携者（BA）内における故意でない、誠実なアクセスもしくは開示は例外となる
- 暫定的最終規則（IFR）データ漏えい通知基準
  - 暫定的最終規則（IFR）：適用主体（CE）／事業提携者（BA）は、データ主体に危害が及ぶ重大なリスクを引き起こす、安全でない保護対象保健情報（PHI）の漏えいを通知しなければならない
  - 危害には財務およびその他の危害が含まれるが、基準には議論の余地があった
  - NISTの基準に準拠して正しく暗号化されたデータは、安全でない保護対象保健情報（PHI）に該当しない
  - 例外には、追加的な削除により制限されたデータセットが含まれていた

米国HIPAA／HITECH総括規則の動向

米国HIPAA／HITECH総括的規則と個人の権利（2）

- 暫定的最終規則（IFR）データ漏えい通知基準（続き）
  - 「漏えい」の定義は、暫定的最終規則（IFR）の定義から変更される
  - 適用主体（CE）／事業提携者（BA）が、保護対象保健情報（PHI）に危害が及ぶ可能性が低いことを示さない限り、容認できない保護対象保健情報（PHI）の利用／開示は、漏えいと推定される
  - データに危害が及ぶ可能性が低いか否かを決定するためには、データに何が起きたか（何が起きる可能性があったか）を分析する必要がある
  - 制限されたデータセットの例外は削除された

米国HIPAA／HITECH総括規則の動向

- 米国HIPAA／HITECH総括的規則と個人の権利（3）
  - データ漏えい通知とリスク評価
    - 適用主体（CE）／事業提携者（BA）は、漏えい後の調査においてリスク評価を行う際に、以下の点を考慮しなければならない
      - 識別子のタイプ、再識別の可能性など、含まれている保護対象保健情報（PHI）の性質や範囲
      - 誰が保護対象保健情報（PHI）の受け手であったか
      - 保護対象保健情報（PHI）は、実際に取得もしくは閲覧されたか
      - 保護対象保健情報（PHI）を誤用するリスクはどの程度軽減されたか
  - データ漏えい通知と立証責任
    - リスク評価が実施されていなければ、デフォルトは通知
    - 保護対象保健情報（PHI）に危害が及ぶ可能性が低いことを示す責任は、適用主体（CE）／事業提携者（BA）にある
    - 通知しないという決定については、レビュー時に文書化されなければならない

米国HIPAA／HITECH総括規則の動向

- 米国HIPAA／HITECH総括的規則と個人の権利（4）
  - データ漏えい通知に関する責務
    - 適用主体（CE）は、個人に通知しなければならない（事業提携者（BA）にこれを委託することは可能であるが）
    - 事業提携者（BA）は、適用主体（CE）に通知しなければならない
    - 下請け事業者は、情報が連鎖を遡れるよう、契約パートナーに通知する義務がある

米国HIPAA／HITECH総括規則の動向

米国HIPAA／HITECH総括的規則と個人の権利（5）

リスク分析項目（例）

分析項目	分析対象	評価（例）
識別／再識別の可能性	患者名リスト	可能性は低くない
	特定化できない患者退院データー患者の再識別は可能か？	低い可能性がある（状況による）
誰が権限のない受け手か	HIPAA適用主体	リスクが軽減された証拠がある限り、可能性は低い
	雇用者 - 再認識のために個人記録を利用する可能性がある	可能性は低くない
実際に入手／閲覧された保護対象保健情報（PHI）	ラップトップで改ざんされていない	可能性は低い
	間違った人に送付した情報	可能性は低くない
不適切な利用が軽減されたか	既知の人からの破壊に関する十分な保証	可能性は低い

米国HIPAA／HITECH総括規則の動向

- 米国HIPAA／HITECH総括的規則と個人の権利（6）
  - データ漏えい通知に関して、HIPAA／HITECH総括的規則施行前と変わらない点
    - 「安全でない保護対象保健情報（PHI）」の定義
    - 漏えいが「発見された」と取り扱われる時点
    - 通知のタイムライン
    - 通知の内容
    - 通知の方法
    - メディアおよび当局への通知（部分修正－発見の年から数える）
    - 事業提携者（BA）による通知
    - 法の執行によって要求された遅延
    - 文書化と立証責任
    - 州法に関する優先権の基準

米国HIPAA／HITECH総括規則の動向

電子保健情報に対する患者のアクセス（1）

- 保護対象保健情報（PHI）が電子的に保存されている場合、個人は「指定されたレコードセット」（「電子健康記録（EHR）」の情報にとどまらない）で電子コピーを入手する権利がある
- 「すぐ提出できる」場合、要求されたフォーマットで提出する。そうでない場合、主体と個人の間で同意した判読可能な電子フォーム／フォーマットで提出する
  - このために、新たにソフトウェアを購入する必要はないが、電子コピーを提供する能力を有しなければならない
  - もし、主体が提供可能な電子フォーマットを受諾しない場合、ハードコピーをデフォルトとすることができる
  - 患者のデバイスを受け入れる必要はないが、望まない場合、個人にデバイスの購入を要求することはできない

米国HIPAA／HITECH総括規則の動向

- 電子保健情報に対する患者のアクセス（2）
  - 合理的な予防手段
    - 電子化された保護対象保健情報（PHI）の交換を保護するために、合理的な予防手段を講じる必要がある
      - もし個人が暗号化されていない電子メールで情報の入手を希望する場合、主体は、このような交換にはリスクがあることを助言した上で、送付することができる
      - 安全なメカニズムを有する必要があり、安全でない状態を受け入れるよう強いることはできない

米国HIPAA／HITECH総括規則の動向

- 電子保健情報に対する患者のアクセス（3）
  - 第三者機関、提供費用
    - 個人は、他の人／主体に直接コピーを提供させることができるが、書面で選択し、個人／主体を明確に特定する必要がある
      - 情報は保護されている必要があり、主体は、合理的なポリシー／手順を導入し、正しい場所に送付する必要がある（例．正確に電子メールを入力する）
      - 「書面で」は電子化することができる
    - 徴収する費用は人件費に限定され、修復費用や資本コストの部分を含めることはできない
    - 料金には、個人の要求に基づいて提供された消耗品を含めることができる

米国HIPAA／HITECH総括規則の動向

- 保護対象保健情報（PHI）のマーケティング利用（1）
  - HITECH施行前
    - プライバシー懸念に関する公的調査で、データのマーケティング利用（特に健康その他の機微なデータ）が上位に位置づけられている
    - HITECH施行前：保護対象保健情報（PHI）のマーケティング利用には、事前に患者の許諾を得ることが要求された。ただし、適用主体（CE）が、処置のため、もしくは追加的な利得やサービスを推奨するために送付した通信は、マーケティングに該当しなかった

米国HIPAA／HITECH総括規則の動向

保護対象保健情報（PHI）のマーケティング利用（2）

HITECH包括的規則施行後

- 規則制定案告示（NPRM）からの重要な変更：適用主体（CE）／事業提携者（BA）が、マーケティングコミュニケーションを行うことによって、製品／サービスが設定された第三者から金銭的報酬を受け取る場所で、保護対象保健情報（PHI）を利用／開示するためには、患者からの事前許諾が必要となった。
- 規則制定案告示（NPRM）における処置のためのコミュニケーションと「業務」のためのコミュニケーションの区別が廃止された。
- 製品／サービスを適用主体（CE）／事業提携者（BA）に提供する製造業者若しくはその代わりが金銭的報酬を提供する場合、コミュニケーションはマーケティングに該当し、者からの事前許諾が必要となる。
- 許諾の際、コミュニケーションに報酬が支払われることを開示しなければならない
- 適用主体（CE）は、このようなコミュニケーション全てに適用される一般的な許諾を利用することも、ケースバイケースで許諾を取ることも可能である

米国HIPAA／HITECH総括規則の動向

- 保護対象保健情報（PHI）のマーケティング利用（3）
  - マーケティングの例外
    - 補充通知状の例外
      - 報酬は、現在処方されている医薬品／生物由来製品（後発品含む）に認められる
      - 報酬は、コミュニケーションを行う費用に、相応に関係するものでなければならない（利益を上げることはできない）
    - 対面コミュニケーションは例外であり、合理的な報酬（人件費、消耗品、郵送費）について要件はない
    - 適用主体（CE）によって提供される、わずかばかりの価値の販促ギフトから成るコミュニケーションは例外である

米国HIPAA／HITECH総括規則の動向

- 保護対象保健情報（PHI）のマーケティング利用（4）
  - 金銭的報酬の対象範囲
    - 直接、間接の支払いは計上されるが、物品による便益は計上されない
    - 支払いは、マーケティングコミュニケーションを行うためになされる。プログラム導入（疾病管理プログラムなど）のための支払いは、マーケティング許諾要件の契機とはならない
      - ただし、コミュニケーションはプログラムへの参加を促すものであり、第三者の製品／サービスの利用／購入を促すものではないという前提に立っている。
    - 公的プログラムの資格に関わる一般的な健康増進／コミュニケーションは、公的援助を受けたものであっても、マーケティングには該当しない

米国HIPAA／HITECH総括規則の動向

- 保護対象保健情報（PHI）のマーケティング利用（5）
  - ファンドレイジング
    - ファンドレイジング―適用主体をプロモートするための保護対象保健情報（PHI）利用（第三者に便益をもたらす目的ではない）
    - 拡張されたタイプの保護対象保健情報（PHI）をファンドレイジングに利用することは可能（サービス部門、かかりつけ医、アウトカムなどが含まれる）
    - 明確で目に付くオプトアウトで、敬意を表したものである必要がある
    - 初期のコミュニケーションにおけるオプトアウトの通知が可能であり、包括的なオプトアウトでもよい
    - 患者の意思決定による処置を条件とすることはできない

米国HIPAA／HITECH総括規則の動向

保護対象保健情報（PHI）のマーケティング利用（6）

- 保護対象保健情報（PHI）の販売
  - 一般的に許諾が必要であり、金銭と交換で保護対象保健情報（PHI）が開示されることを通知しなければならない（金銭以外の便益も含まれる）
- 販売の例外
  - 公衆衛生
  - 研究目的～報酬は、情報の準備および交換する費用に見合ったものである必要がある（間接費用を含めることは可能であるが、利益を上げてはいけない）
  - 処置と支払い～支払いを受け取るための保護対象保健情報（PHI）開示は、保護対象保健情報（PHI）の販売には該当しない
  - 法人取引
  - 事業提携者（BA）に対する開示
  - 個人に対する開示
  - 法律に要請された開示
  - その他規則によって認められた開示で、提供される報酬が開示を行う費用に関連したもの

米国HIPAA／HITECH総括規則の動向

- 保護対象保健情報（PHI）の研究利用
  - 研究
    - 研究者は、HIPAAおよび共通規則の変更によって、研究目的のデータ利用への道が緩和されると考えていた
    - 共通規則の行政立法事前通知（ANPRM：Advance Notice of Proposed Rulemaking）は2011年7月に公表
    - 総括的規則には、いくつかの条項が含まれる：
      - 研究目的の保護対象保健情報（PHI）の移転に対する報酬は認められる（費用に基づく合理的な料金である必要がある）
      - 複合的な許諾は認められる
      - 許諾は、研究に特化したものである必要はない：将来の研究利用の記述が十分明確であり、このような将来の研究のために、個人の保護対象保健情報（PHI）が利用／開示されることが合理的であると考えられる限り、将来の研究に対する許諾は可能である

米国HIPAA／HITECH総括規則の動向

- 保険者とのデータ共有の制限を要求する権利
  - プロバイダーに適用される
  - 要求があれば、保護対象保健情報（PHI）を強制的に非開示
    - 特定の保健サービスのための全額自費負担
    - 医療保険制度の下で、年間控除の要件を満たさない
  - 全てか無の規則を押し付けることはできない（支払いがまとまっていれば、患者に対しては、一括で支払うよう指導される）
  - 患者がフォローアップのために自費で支払いたくない時は、フォローアップケアの支払いを支援するために情報を開示できる
  - 内部のメカニズムが機能していない場合（例．不渡小切手）、患者から適切な支払いを得るために努力しなければならない、

米国HIPAA／HITECH総括規則の動向

プライバシー保護方法の通知（NPP）

- プライバシー保護方法の通知（NPP：Notice of Privacy Practices）には、下記が含まれなければいけない：
  - （a）許諾を必要とする特定の利用／開示に関する言明
    - 例．心理療法記録（適当なところで）、マーケティング、PHIの販売、医療保険者に対する開示を制限する権利（プロバイダーのみ）、漏えいの通知を受ける権利
  - （b）NPPに記載されていない利用／開示全てに対して許諾を必要とする旨の一般的言明

総括的規則－NPPを修正する必要がある

- 規則における変更点は資料である
- Webサイト上で告知した保険者の場合、施行日までに、次の年次通知で修正したNPPを告知する
- Webサイトがなければ、保険者は60日以内に修正版資料を提供しなければならない
- プロバイダーは、要求に応じて、告知／提供しなければならない；新しい患者に提供しなければならない（そして承認を得なければならない）
- もし個人が同意すれば、電子メールで送付することができる

米国HIPAA／HITECH総括規則の動向

- 遺伝子情報－GINA
  - 医療保険および雇用における遺伝子による差別を禁止
  - 規則においては、以下のような手順で、遺伝子情報差別禁止法（GINA：Genetic Information Nondiscrimination Act of 2008）を導入する：
    - 遺伝子情報（GINAにより定義）が 保護対象保健情報（PHI）であることを宣言する
    - HIPAAの適用対象となるほとんどの医療保険者に対し、引き受けのために遺伝子情報である保護対象保健情報（PHI）の利用／開示を禁じる
    - 保険者は、受益者に対し、NPPにおけるこの制限を告知することが求められる
  - 長期医療保険者に関しては例外があり、遺伝子情報を引き受けに利用することができる

米国HIPAA／HITECH総括規則の動向

- 執行規則
  - 2009年2月18日付のHITECHの下で施行された執行規則が、執行暫定的最終規則（IFR：Interim Final Rule）（2009年10月30日）を受けて修正される
  - HITECH規則制定案告示（NPRM：Notice of Proposed Rulemaking）（2010年7月14日）が、IFRにより修正された通り執行規制に修正を加えることを提案
  - 総括的規制：法令遵守、調査、罰則について修正
- 執行規則：事業提携者（BA）、調査、レビュー
  - 民事制裁金（CMPs：Civil Monetary Penalties）を直接、事業提携者（BA）に課することができる
  - 不服申し立てに基づく調査とコンプライアンスレビュー
    - 故意に怠ったために、HIPAA違反の可能性を示す証拠があった場合に要求される
    - 故意に怠った可能性がない場合は、自主的判断による
    - 全ての不服申し立てについて、あらかじめ調査しなければならない
    - 規制当局は、非公式の解決なしに、民事制裁金（CMPs）を直接課することができる

米国HIPAA／HITECH総括規則の動向

- 執行規則：調整
  - 規制当局は、要求に応じて、保護対象保健情報（PHI）を他の省庁に開示することがある
  - 司法省と連邦取引委員会（FTC）の調整
  - 直接執行の支援を目的とする司法長官との調整
- 執行：民事制裁金（CMPs）
  - 執行暫定的最終規則（IFR）から持ち越された3段階の罰則
    - 知らなかった場合：100ドル～5万ドル
    - 合理的な理由がある場合：1,000ドル～5万ドル
    - 故意に怠り、修正した場合：1万ドル～5万ドル
    - 故意に怠り、修正しなかった場合：5万ドル
  - 年間の上限：違反の一類型当たり150万ドル
  - 新たな「合理的な理由」の定義で、心理状態に言及：違反であることを知っていたが、故意に怠ってはいなかった
  - 「故意に怠る」の定義は維持：「意識した、意図的な失敗もしくは無謀な無関心」

米国HIPAA／HITECH総括規則の動向

- 執行規則：民事制裁金（CMPs）と代理人の責務
  - 適用主体（CE）／事業提携者（BA）およびその請負事業者は、代理人のHIPAA違反の責務を負う
  - 連邦訴訟法の適用：当局の所管範囲内で代理人が起こした行為に対する本人の責務
  - 特別な決定の事実：本人は、契約上のサービスを実行する際に代理人の行為をコントロールしていたか、コントロールする権利があったか、指揮していたか？
  - 本人が実際にコントロールするサービスで提供された方法や手段が決定的

米国HIPAA／HITECH総括規則の動向

- 執行規則：民事制裁金（CMPs）の留意点
  - 公民権局（OCR:Office for Civil Rights）は以下の点を考慮する予定である
    - 違反の性質と程度
    - 物理的、金銭的、名声的被害の性質と程度
    - 適用主体（CE）／事業提携者（BA）が過去に法令を遵守していなかった履歴
    - 適用主体（CE）／事業提携者（BA）の財務状況
    - 裁判で要求されるその他の要因
      - 名声その他の被害の程度
      - 違反が発生していた期間
      - 影響を受けた個人の数

米国HIPAA／HITECH総括規則の動向

- 執行規則：民事制裁金（CMPs）に対する積極的抗弁
  - 反がHIPAAの刑事罰規定に基づいて罰するに値する場合、2011年2月18日以前に発生した違反について民事制裁金は科せられない
  - 2011年2月18日以降に発生した違反について、HIPAAの刑事罰規定に基づいて罰則が科せられた場合、民事制裁金が科せられない可能性がある
  - 2009年2月18日以前に発生した違反について、下記のような場合、民事制裁金が適用主体（CE）に科せられない可能性がある
    - 適用主体（CE）が違反の認識がなく、相当な注意を払う訓練を行っていたとしてもなかったであろうことを証明できる場合
    - 違反が以下のような状況に起因する場合
      - 遵守することが合理的でなかった場合
      - 故意に怠ったためでない場合
      - 違反を知った時もしくは知るべき時から30日以内に是正された場合
  - 2009年2月18日以降に発生した違反に対しては、事業提携者（BA）に拡張される形で同様の基準が適用される

米国HIPAA／HITECH総括規則の動向

- 次のステップ
  - ポリシー、手順、様式を見直して更新する
  - スタッフに対して新たな規則に関するトレーニングを行う
  - 業提携者（BA）の棚卸をして、事業提携契約書（BAA）を更新する
  - 情報漏えい対策計画を更新する；特にリスク評価を更新し、暗号化に取り組む
  - 先延ばししない

Open Question

【Reference】

“*CSA Cloud Bytes: An Overview of the HIPAA Omnibus Rule*”
(June 13, 2013)

https://cloudsecurityalliance.org/research/cloud-bytes/hipaa-omnibus-rule/