刑事手続における情報通信技術の活用に関する検討会（第５回）

第１　日　時　　令和３年７月２７日（火）　　自　午後１時３１分
　　至　午後３時５３分

第２　場　所　　法務省１階集団処遇室

第３　議　題　　○　進関係官からの説明
　　１　情報セキュリティ対策
　　２　通信サービス・回線の技術及び安全性
　　３　電子データの改ざん防止措置
　　４　その他

第４　議　事　（次のとおり）

議　　事

○仲戸川室長　それでは，ただいまから，刑事手続における情報通信技術の活用に関する検討会第５回会議を開催いたします。

○小木曽座長　皆様，こんにちは。本日もお集まりいただきましてありがとうございます。よろしくお願いいたします。

まず，議事に入ります前に，事務局の担当者に変更がありましたので，自己紹介をお願いいたします。

○仲戸川室長　今月１６日付けで前任の南部室長の後任として刑事局総務課企画調査室長になりました仲戸川でございます。どうぞよろしくお願いいたします。

○小木曽座長　それでは，本日の配布資料について確認をお願いいたします。

○仲戸川室長　本日は，議事次第と共に説明資料をお配りしております。ウェブ参加の皆様におかれましてはお手元に資料の御準備をお願いします。また，法務省の会場で御参加の方につきましては，今申し上げた資料を机上に御用意しておりますので，御確認ください。

なお，この後の進関係官からの御説明の際は，画面の共有機能によりまして，お手元の端末の画面上にも必要に応じて同じ内容の資料が表示されることになりますので，適宜御参照ください。

○小木曽座長　ありがとうございます。

それでは，説明と意見交換に入りたいと思います。

本日は，予定しておりましたとおり，政府ＣＩＯ補佐官・法務省ＣＩＯ補佐官でいらっしゃる進京一関係官から御説明を頂戴することにいたします。進関係官からは，一巡目の議論で示された課題に関連しまして必要な範囲で技術面に関する御説明を頂き，これに続いて質疑応答・意見交換を行うことにしたいと思います。

具体的には，進関係官からの御提案によりまして，全体を「１　情報セキュリティ対策」，「２　通信サービス・回線の技術及び安全性」，「３　電子データの改ざん防止措置」の三つに分け，それぞれのテーマごとに，まず御説明いただいて，その上で質疑応答・意見交換を行うことにしたいと思います。その後で，「その他」としまして，「１」から「３」までのテーマに含まれない事柄について御質問や御発言があれば意見交換を行うことにしたいと思います。

それでは，まず「１　情報セキュリティ対策」についての御説明をお願いしたいと思い

ます。

進関係官，よろしくお願いいたします。

○進関係官　ＣＩＯ補佐官の進でございます。本日は御説明をさせていただきます。どうぞよろしくお願いいたします。

本検討会におきましては，刑事手続に情報通信技術を活用することによって効率化，非対面・遠隔化等を図るための方策の在り方について検討がされており，私は，技術的観点から助言をする役割の関係官という立場で本検討会の検討に参加させていただいているところでございます。前回会議までに全論点についての一巡目の議論が行われましたが，その中で技術的な事項についても課題が指摘されておりますので，本日はそのような課題に関連して，私から技術的観点から必要な説明をすることとさせていただきます。

なお，私は刑事手続における情報通信技術の活用方策の在り方について直接意見をすべき立場にはないことから，指摘されている課題に関連して，現状においてどのような技術が利用されているのかや，それら技術のメリット・デメリットは何かなどといった，飽くまで技術的観点から一般的な説明をするにとどめることとしたいと考えております。その点について御了承いただきたいと存じます。

それでは，説明に入らせていただきます。本検討会の一巡目の議論で指摘された技術的な事項に関する課題については，主要なものとして，「情報セキュリティ対策」，「通信サービス・回線の技術及び安全性」，「電子データの改ざん防止措置」に分類できると思われるため，先ほど座長からもお話があったとおり，これらの項目について順次説明させていただくことといたします。

それでは，まず一つ目のテーマとして，「情報セキュリティ対策」について御説明いたします。検討会においては，各委員から，刑事事件で取り扱う情報は非常にプライバシー性が高いものであるから，従来紙媒体で作成してきた書類を電子データで作成することとし，そのやり取りをオンラインで行うに当たっては，十分な情報セキュリティを確保することが必要になるとの御意見がございました。そこで，本検討会での議論に資するよう，情報セキュリティを確保するための技術について，その概要を説明することといたします。

まず，情報セキュリティ対策を考える前提として，情報漏えいの主な脅威について御説明いたします。なお，一般に，情報セキュリティについては，機密性・完全性・可用性の３要素が重要とされておりますが，各委員からは特に情報漏えいについての懸念が示されていることから，ここではセキュリティの３要素のうち，機密性，つまり，情報漏えいを

防止する点を中心に御説明いたします。

御覧いただいておりますスライド（スライド３枚目）は，一般的な企業において想定され得る情報漏えいの主な脅威を表したものでございます。このスライドの中央にある「社内ネットワーク」がさらされる情報漏えいの主な脅威について，外部からの脅威及び内部からの脅威に分けて御説明いたします。

まず，スライドの左側の「外部」と書かれた緑色の部分を御覧ください。外部からの脅威の一つ目としては，「マルウェア感染」が挙げられます。マルウェアとは，ウイルスやトロイの木馬などに代表される不正かつ有害な動作を行う意図で作成された悪意のあるソフトウェアや悪質なコードの総称です。コンピュータがマルウェアに感染すれば，コンピュータ内にあるファイルが消されたり，改ざんされたり，外部ネットワークに漏えいするといった事態に陥る危険がございます。マルウェアは一般的にはインターネットを通じて社内ネットワークに侵入してくるものであり，具体的には，ソフトウェアのぜい弱性を悪用する手口や，電子メールにウイルスを添付して送付する手口など，様々な手口により内部ネットワークに侵入する例が確認されております。なお，インターネットを通じた侵入だけでなく，汚染されたＵＳＢメモリ等の記録媒体を介して社内ネットワークに侵入する場合もございます。

次に，外部からの脅威の二つ目としては，「なりすまし等による不正ログイン」によるリスクが挙げられます。これは，社内ネットワークの利用者が利用しているＩＤやパスワード等が窃取され，又は推測されることにより，不正なログインがされるリスクです。不正ログインにより生じる被害は，インターネット上のサービスの機能に応じて様々なものが考えられます。例えば，攻撃者が何らかの方法で従業員のＩＤとパスワードを入手し，従業員になりすましてサービスに不正にログインし，取引先の名称やその金融機関口座等の情報を流出させた事例などが確認されております。

次に，外部からの脅威の三つ目としては，「送付先端末のマルウェア感染」が挙げられます。外部からの脅威を防ぐために自らの組織のセキュリティをいかに堅牢なものとしたとしても，取引先など電子データを送付する先の端末や送付先の社内ネットワークがマルウェアに感染したり，なりすまし等による不正ログインがされることがあれば，それら送付先から情報が漏えいする事態が生じ得ます。実際，サイバー攻撃の攻撃者は，ある特定の企業を攻撃するに当たり，当該企業が電子データのやり取りをする取引先等のうちセキュリティがぜい弱なところを攻撃の足掛かりとする手口を用いることがあると言われてお

ります。このような手口が用いられれば，幾ら社内ネットワークのセキュリティを堅牢なものとしたとしても，セキュリティがぜい弱な取引先等から自らの組織の情報が漏えいしてしまうこととなります。

次に，スライドの右側の「内部」と書かれたオレンジ色の部分を御覧ください。組織内部の従業員は重要情報にアクセスしやすいことから，例えば，悪意を持った内部者がＵＳＢメモリ等を使って情報を抜き取ったり，ＰＣの画面をスクリーンショットしたり，スマートフォンのカメラで写真撮影したりするなどして，内部の重要情報が不正に持ち出され，漏えいするリスクがございます。また，悪意を持った内部者による情報漏えいだけでなく，内部者が過失により外部に電子データを誤送信するなどにより，内部の情報が漏えいするリスクもございます。

以上が，考えられる情報漏えいの主な脅威についての説明でございます。

次のスライド（スライド４枚目）でございますが，御覧いただいているスライドは，システムの堅牢性のための情報セキュリティ対策を表したものです。セキュリティ対策には大きく分けて二つのモデルがございます。一つは，スライド左側，「境界防御型モデル」と呼ばれているものです。これは，ネットワークの内部は定常的に安全であるという前提の下，社内ネットワークと，インターネットなど外部ネットワークとの間に，ファイアウォール等の境界を設け，外部から内部への不正な侵入を遮断することで，社内ネットワークのセキュリティを確保しようとするものです。

もう一つは，スライド右側の「ゼロトラストモデル」と呼ばれているものです。ゼロトラストモデルは，クラウドサービスやテレワークが普及したことなどにより，保護すべき電子データが境界の外側であるインターネット上など様々な場所に点在するようになったことで，内部と外部との境界が曖昧になったことをきっかけとして，情報セキュリティ対策のモデルとして新たに提唱されるに至った考え方です。ゼロトラストモデルは，「ゼロトラスト」，すなわち，全ての端末や通信を信用しないという前提の下，内部・外部を問わず，全てのアクセスに対し認証・認可を行うことや，ネットワークやそれに接続される各種デバイスの管理，これらの統合的なログの収集・分析による監視，多要素認証の利用などによるユーザー認証の強化，通信経路の暗号化などによりセキュリティを確保するものでございます。

このように，情報セキュリティ対策には大きく二つのモデルがございますが，ここで重要なことは，この境界防御型モデルとゼロトラストモデル，この二つがそれぞれ相反する

ものではなく，その二つが共同の立場で使われるべきだという点にございます。例えば，現在も，多くの企業や省庁において，セキュリティ対策として，ファイアウォール等の境界型防御を設けるというセキュリティ対策をしつつ，従業員ごとにアクセス権限を定めて社内のデータにアクセスできる範囲を限るゼロトラストモデルのセキュリティ対策を施している例が多いものと思われます。今後も，情報セキュリティを確保する方法としては，一般に境界防御型モデルとゼロトラストモデルを併用するなど，双方のメリットをいかしていくことが多いのではないかと思われます。

以上がシステムの堅牢性のための情報セキュリティ対策についての説明でございます。

次に，外部に電子データを送信する場面における情報セキュリティ対策について御説明します。ここでは，御覧いただいているスライド（スライド５枚目）の左側にある「作成元」と書かれた企業が，スライド中央の「送付先」と書かれた企業に対して電子データのファイルを送信する場合に，当該ファイルが送付先から漏えいすることを防止するために用いられる技術を紹介いたします。

前提として，組織の外部との電子データのやり取りには，外部への送信だけでなく外部からの受信もございますが，外部から電子データを受信する場面においては，組織のセキュリティを堅牢にし，外部から内部へ入ってくるデータのチェックを厳格に行うことで内部システムを保護するという対策が可能でございます。

他方で，電子データの送信の場面においては，３枚目のスライドでも御説明いたしましたように，組織のセキュリティをいかに堅牢なものとしたとしても，外部に送信した電子データについては自らの組織のセキュリティや監視が及ばないという問題がございます。そのため，送付先のシステムがマルウェアに感染し，あるいは不正アクセスされ，送付したファイルが漏えいするおそれ，送付したファイルを送付先の従業員が外部に持ち出すおそれ，送付先の従業員が宛先メールアドレスを間違えるなどして意図しない人にファイルを送信されるおそれなどのリスクがございます。

このようなリスクを防止するための技術として一般的に広く用いられているのが，「データの暗号化」です。データを暗号化すれば，パスワードなどにより復号されない限りファイルの内容を閲覧することができなくなることから，仮に送付先から第三者にファイルが漏えいしたとしても，その閲覧を防ぐことができます。もっとも，作成元が送付先の特定の人物にだけ復号を許可するつもりでファイルとパスワードを送信したとしても，送付先の人が別の者にパスワードと共に当該ファイルを渡せば，その後，誰がファイルを復号

しているか把握することが不可能となってしまいます。その結果，このように拡散したファイルとパスワードが，セキュリティがぜい弱なところから漏えいする，何者かがインターネット上にパスワードと共にファイルを公開するといったような事態も生じかねません。

このような情報漏えいを防止するための技術として，暗号化の際に「アクセス権限設定」によりファイルを保護する等の技術がございます。このアクセス権限の設定により，作成元が閲覧を許可した特定の者だけにファイルの開封を可能とすることができ，それ以外のアクセス権限のない者が閲覧しようとしても開封できないようにすることができます。この技術を用いれば，外部に送信した電子データの流出を防ぐことができ，作成元がデータ共有したい相手との間だけでデータ共有を図ることが可能となります。

以上が，外部に電子データを送信する場面における情報セキュリティ対策についての説明でございます。

情報セキュリティ対策についての私からの説明は以上でございます。

○小木曽座長　ありがとうございました。

それでは，ただいまの御説明を踏まえまして，質疑応答・意見交換をいたしたいと思います。どなたからでも御発言をお願いいたします。

○吉澤委員　３枚目のスライドに関しまして，右側の内部からの情報漏洩のカテゴリーのうち，「内部者がスクリーンショット，写真撮影」という点なのですが，ここに関して，スクリーンショットに関してはちょっと調べてみましたら，例えば，パソコンの画面などで機能制限をするということが可能ということが分かったのですけれども，カメラで写真撮影をする，それ自体を防ぐとか，あとは，防ぐのと同じような結論を得られる，例えば写真撮影をしても，その画像なり動画なりが画像や動画として確認できないとか，そういうような形で制限を掛けるということは技術的に可能なのでしょうか。教えていただければと思います。

○進関係官　スクリーンショットや写真撮影による漏えいを防ぐためには，第一に考えられる対応策は，従業員のアクセス権限を適切に管理する方法でございます。機密情報にアクセス可能な従業員の範囲を厳格に定めることにより，情報漏えいのリスクを低減することができます。その上で，機密情報について，例えば画面の透かし，それから印刷透かしの技術を用いて，画面上や印刷面上にユーザーＩＤなどを表示させることにより，スクリーンショットや写真撮影・印刷を心理的に抑止することができるとともに，仮に漏えいしたとしても漏えいした者を特定することが可能となるというような方法がございます。さら

に，スクリーンショット等による情報漏えいを心理的に抑止するとともに，被害を早期に検知することができるよう，システム操作履歴の監視をすることなどが考えられます。

○吉澤委員　今おっしゃっていただいたシステム操作履歴の監視ですけれども，これはキャプチャ画面というか，このスクリーンショットに関しては可能かと思うんですが，写真で撮影するということは，やはり監視はできないということでよろしいでしょうか。

○進関係官　そうですね，履歴そのものは，その画面をある時間に見ていたということは分かると思います。それから，先ほど透かし等のお話をしましたが，画面上にＩＤや，例えば時刻，そういうものを映すことによって，もちろんその画像そのものを編集されてしまえば情報がなくなるわけですけれども，まず第一義的に，編集する前でしたら，その部分で特定するというようなこともできますので，それによって，更に心理的抑制になるのではないかというふうに考えられます。

○吉澤委員　あと１点だけ，すみません。透かしということを教えていただきましたが，例えば，透かしというふうに一般的に言いますと，もともとの画面は見える上に透かしというか，その上に更に別の文字情報などを乗せることかなと思うのですが，例えば，写真撮影をしたりとかスクリーンショットを撮ったときに，その画面自体が，例えば真っ黒というか，極端な話，そのような形で画面自体が全く確認できなくなるような形にするというのは可能なのでしょうか。

○進関係官　今は余り一般的には使われていないと思いますけれども，例えば，特殊な画面として，フィルターを幾つも掛けて，そのフィルターを置換操作することによって，例えばそのフィルターに対応する電子眼鏡を掛けている人にしかその画像が見えないといったような技術はいろいろ研究されているというふうに伺っております。もちろん，そのようなものをどの場面でお使いになるのかというのはあるのかもしれませんが，例えばそういうことですと，そのフィルターを付けていないカメラで撮ってもその画面は見えないというような技術はあるように聞いております。

○成瀬委員　今，吉澤委員から内部の脅威について御質問がございましたが，私は外部の脅威について質問させていただきたいと思います。先ほどの御説明では，マルウェア感染やなりすまし等による不正ログインがあるとのことでしたが，これらの脅威に対して，どのような対応策が考えられるのでしょうか。御教示いただければ幸いです。

○進関係官　情報セキュリティのリスクは時代に応じて変化するものでございまして，近年ではランサムウェアによる被害やテレワーク等のニューノーマルな働き方を狙った攻撃に

よる被害が目立っております。もっとも，攻撃の内容が変化してもこれらの攻撃の糸口は似通っておりまして，基本的なセキュリティ対策を施すことが最も重要であるというふうにされております。

対応策ということの御質問でございますけれども，具体的には，ソフトウェアのぜい弱性を糸口にした攻撃に対しては，ソフトウェアの更新によりぜい弱性を解消し攻撃によるリスクを低減する方法，ウイルスの感染を糸口とした攻撃に対しては，セキュリティソフトを利用することによりウイルスの侵入を防ぐ方法，パスワード窃取を糸口とした攻撃に対しては，パスワードの管理・認証の強化をすることによりパスワード窃取によるリスクを低減する方法，クラウドサービス等の設定不備を糸口とした攻撃に対しては，設定を適切に見直すなどにより誤った設定を攻撃に利用されないようにする方法といったように，基本的な対策を徹底することが重要であるというふうに考えております。

○佐久間委員　先ほど，外部に送信されたデータの漏えいを防ぐための技術的措置に関する御説明を頂きました。その御説明によれば，アクセス権限を設定する技術を用いるとのことでしたが，この技術では具体的にどのような方法によって電子データの漏えいを防止することができるのかについて，更に御説明いただけないでしょうか。

○進関係官　外部に送信した電子データの漏えいを防ぐための技術的措置として，暗号化の際にアクセス権限を設定してファイルを保護する技術を御説明いたしました。アクセス権限設定の技術というのは，概要としましては，ファイルを開封するなどの操作の都度，当該ファイルがアクセス権限管理サーバにアクセスして，当該ファイルに認められた操作を確認し，作成元が許可した操作のみを送付先に認める技術というようなものでございます。

アクセス権限設定において設定することができる権限としましては，ファイルの開封権限だけではなく，ファイルに対しての様々な操作権限でございまして，具体的には，暗号化の解除の権限，更新の権限，印刷の権限なども設定可能であるというふうに聞いております。今，アクセス権限管理サーバという表現をいたしました。アクセス権限設定の技術の性質上，ファイルがアクセス権限管理サーバにオンラインでアクセスする必要があるのが今の技術の原則でございます。さらに，オフラインであっても一定のセキュリティ上の制限，今のようないろいろな権限ではなく，ある一定の権限といったような形で使用できるような技術があるというふうに聞いております。

○佐久間委員　ありがとうございました。

○小木曽座長　ほかに御質問はいかがでしょうか。御質問がなければ，御意見でも結構です

が。

○笹倉委員　では，若干意見を申し上げます。これまでの会合で私自身も述べてきたことですけれども，刑事事件で取り扱う情報は一般にプライバシー性が極めて高く，これが漏えいすることは厳に避けなければならないところです。ただいま進関係官もそのことを大前提として御説明を頂いたところです。

漏えいを防止するためには，まず，刑事事件に係る情報を多く管理する裁判所や検察庁，さらに，警察を始めとする司法警察職員が所属する機関が構築するシステムについて，高い堅牢性を備えたものとすることが重要となると考えます。もちろん弁護士の方々におかれても，それぞれの法律事務所において堅牢なセキュリティを構築されることが重要となります。

ただいまの進関係官からの御説明を伺いまして，情報通信技術を活用するに当たっては，境界防御型の考え方とゼロトラストの考え方の双方を組み合わせてセキュリティ対策を施すことにより，自らの組織のセキュリティの堅牢性を高めていくことができるということがこの場の共通理解になったと考えます。

他方で，それぞれの機関が自らのシステムについてセキュリティをいかに堅牢なものとしたとしましても，閲覧や謄写の場面など，それぞれの機関から外に電子データを出す場面においては，提供先，提供相手から情報が漏えいしないような技術的な担保が必要になります。この点についても，ただいま進関係官から，外部に電子データを提供する場面におけるセキュリティ確保の技術として，アクセス権限設定の技術など，様々な御説明があったところであり，このような技術の活用により，外部に提供した電子データが提供先から漏えいしないことを技術的に担保することは可能であろうと考えます。

吉澤委員から，カメラ画面の写真を撮られたらどうなるのかという御懸念が示されました。その御懸念はごもっともですけれども，紙媒体の場合も同じ問題は起こるわけでして，これは電子化に固有の問題ではありませんから，今までやってきたのと同じような対策を取ることで対処できる部分もあるでしょうし，さらに，先ほど御説明があった，フィルターを何重にも掛けるという技術のように，電子化によって保護が高まる場合もあり得るのであれば，写真を撮られる可能性があること自体が直ちに電子化一般を妨げる理由にはならないのであって，電子化は行いつつ，想定される弊害についての対処は別に考えることでよいと思います。

刑事手続における情報通信技術を活用するためのシステムの在り方，さらには外部にデ

ータを提供する際のセキュリティ確保については，今後，更に技術が開発されるかもしれませんが，現時点での技術水準によっても情報漏えいを相当程度防ぐ仕組みを構築することは可能であるということを前提に，本検討会で具体的な方策について検討を進めていくこととしてよいのではないでしょうか。

そして，そうだとしますと，様々な手続で情報通信技術を活用するための法改正をするということであれば，情報セキュリティが確保される方法によることを条件とする，そういう規律を設けることが考えられます。

○吉澤委員　先ほど写真撮影などについてお伺いした趣旨について補足させていただきます。閲覧・謄写の場面で閲覧のみ許されるという証拠があるということについてこれまでお話しさせてもらっていたかと思うのですが，そういう謄写は認められない，閲覧のみというものに関しては，今までは検察庁に出向くなどして，その場で見て，何にも記録は残せない，誰かがいるとか，そういうような状況で，証拠を目で見て確認して帰るというような状況だったわけです。それが事務所でオンラインで可能になるということになると，閲覧のみというふうに幾ら言われていても，それを写真で撮ることで実質的に謄写になってしまうのではないかという懸念があるという点で，先ほどお伺いしました。

ちょっと補足させてもらいました。以上です。

○小木曽座長　ありがとうございます。

ほかはいかがでしょうか。

特段，更に御質問・御意見がなければ，先へ進みたいと思いますが，よろしいですか。

それでは，「１」の「情報セキュリティ対策」についての質疑・意見交換は，ここで一区切りといたしたいと思います。

続きまして，「２」の「通信サービス・回線の技術及び安全性」について御説明を頂戴したいと思います。

進関係官，よろしくお願いいたします。

○進関係官　それでは，２番目に進ませていただきます。

本検討会におきましては，電子データにより作成された書類をオンラインで発受する場合や，取調べ・証人尋問などをビデオリンク方式で実施する場合など，論点項目の「１　書類の電子データ化・発受のオンライン化」と，「２　捜査公判における手続の非対面・遠隔化」のいずれについても，通信に係るセキュリティを十分に確保する必要があるとの指摘があったものと認識しております。そこで，本検討会での議論に資するよう，これに

関連するものとして，通信回線の種類とそれぞれの主な特徴について，技術的な観点から概要を御説明いたします。

スライド（７枚目）の表を御覧ください。スライドの１行目でございますが，「種類」の項目で記載していますように，現在，主に利用されている通信サービスや通信回線としては，まず，専用回線，この中には広域イーサネットも含むというふうに考えております，次に，インターネットＶＰＮ，それから，ＳＳＬやＴＬＳにより通信内容が暗号化されたインターネット等があるというふうに考えております。この表にはそれぞれの概要や特徴などを記載しております。

なお，この表においては，分かりやすさの観点から，三つの通信サービスや通信回線だけを御紹介しておりますが，実際にはこれらに限らず様々な種類の通信サービスや通信回線がございます。また，この表に記載した特徴も，個々の通信業者が提供するサービスやオプションの内容によって幅があるものでございます。これらの点について御留意いただきたいと存じます。

それでは，スライドに示しました表のうち左から１列目，「専用回線」について御説明いたします。これは，「概要」のところに記載したとおり，「通信事業者が独自に用意した閉域網を利用した通信方式」です。従前は，拠点間を物理的に一対一で結ぶ回線を引いたものだけを専用回線と呼んでおりましたが，通信事業者が独自に用意した閉域網の中で拠点間を仮想の一対一対応の通信回線で結ぶ広域イーサネットも広義の専用回線と呼ぶことがございますので，このような形で，「専用回線（広域イーサネットを含む）」というように記載してございます。

「回線」の項目を御覧いただくと分かるように，ほかの２種類の通信サービスと比較した，専用回線の最大の特徴は，不特定多数の者が利用するインターネット回線を使用せず，通信事業者が独自に用意している「閉域網」を使用するという点にございます。専用回線のメリットとしては，「セキュリティ」の項目にあるように，拠点間を結ぶ回線が外部から物理的あるいは論理的に独立していることから，セキュリティの強度が高いことが挙げられます。論理的というのは，通信事業者が用意した閉域網の中で論理的に独立した複数の回線として取り扱うことで，仮想的に一対一対応の通信となるようにしていることを表現してございます。また，閉域網を使用していることのメリットとして，「通信品質」の項目にあるように，通信のための帯域が確保されているため，インターネット回線上の通信の利用状況に左右されることなく高い通信品質を確保することができるという点が挙げ

られます。さらに，「可用性」の項目に「高い」と記載しているところでございますが，可用性，すなわち通信システムが停止することなく稼働し続ける稼働率が高いということもメリットとして挙げられます。他方，専用回線のデメリットとしては，「コスト」の項目にあるとおり，一般にコストが高いという点が挙げられます。

次に，スライドに示した表の中央に記載した「インターネットＶＰＮ」について御説明いたします。これは，「概要」の項目に記載したように，「インターネット回線でＶＰＮ接続を利用した通信方式」です。この次のスライドでＶＰＮについては更に補足いたしますが，このスライドの下の欄外に記載しているように，ＶＰＮ接続とは，ネットワーク上に仮に閉じられたトンネルを作り，接続相手が正しいことを確認しつつ，データを暗号化して送受信する接続方法をいいます。言い換えますと，拠点間を結ぶ仮想のトンネルを構築するとともに，通信の暗号化と，データを送受信する際に送受信者本人であることを確認する認証をすることにより，仮想の閉域網を構築してインターネット回線を使用しつつセキュリティを高める接続方法でございます。ここで仮想の閉域網というふうに申し上げましたけれども，本来は不特定多数の者が利用するインターネット回線の中に，今申し上げたような技術を利用することによって，閉ざされたネットワークを仮に作るということを示してございます。先ほどの専用回線と比較すると，インターネットＶＰＮの特徴は，インターネット回線を使用しつつ，先ほど申し上げたようなトンネル，暗号化，認証の技術を用いてセキュリティを高める点に特徴がございます。

インターネットＶＰＮのメリットとしては，「セキュリティ」の項目では，「仮想の閉域網」と記載しておりますが，インターネット回線の中に仮想のものとはいえ閉域網を構築する通信回線であることから，この次に御説明するインターネットＳＳＬやＴＬＳと比較すると，セキュリティがより確保されているという点が挙げられます。また，「コスト」の項目にあるとおり，専用回線のように拠点間を物理的に結ぶ利用者専用の回線を引いたり，通信事業者が独自に用意した閉域網を利用する必要がないため，専用回線と比べるとコストが低いという点もメリットとして挙げられます。

他方，インターネットＶＰＮのデメリットとしては，専用回線と比較するとセキュリティが劣るという点や，通信事業者が提供する様々なサービスのうちどれを利用するかによっても異なりますけれども，「通信品質」の項目に「ベストエフォート」と記載したとおり，通信のための専用の帯域が確保されていないため，インターネット回線上の通信の利用状況の中で最善の通信品質の確保を試みるといった限度の通信品質しか確保されておら

ず，インターネット回線上の通信の利用状況などによっては通信品質が左右されて安定しないという点が挙げられます。また，「可用性」の項目で記載しているとおり，可用性が閉域網には劣るという点もデメリットとして挙げられます。

最後に，スライドに示した表のうち最も右の列に記載した「インターネット（ＳＳＬ／ＴＬＳ）」について御説明いたします。これは，「概要」の項目に記載したとおり，「インターネット回線を利用し，データを暗号化した通信方式」でございます。身近な例で申し上げますと，ウェブサイトを表示させた際に，ＵＲＬとして「ｈｔｔｐ：／／」ではなく，「ｈｔｔｐｓ：／／」という表記がされるウェブサイトもあるところでございますが，この「ｓ」と表記されているウェブサイトがＳＳＬ／ＴＬＳという通信の暗号化がされているものということになっております。

このメリットとしては，「コスト」の項目に記載したとおり，コストが低いという点が挙げられます。他方，デメリットとしては，「セキュリティ」の項目に記載したとおり，通信データを暗号化するにとどまるため，専用回線やインターネットＶＰＮと比較するとセキュリティが劣るという点や，「通信品質」の項目に「ベストエフォート」と記載したとおり，インターネットＶＰＮと同様，通信のための専用の帯域が確保されていないため，インターネット回線上の通信の利用状況の中で最善の通信品質の確保を試みるといった限度の通信品質しか確保されておらず，インターネット回線上の通信の利用状況などによって通信品質が左右されて安定しないという点が挙げられます。また，「可用性」の項目で記載しているとおり，インターネットＶＰＮと同様，可用性が閉域網には劣る点もデメリットとして挙げられます。

先ほど，「インターネットＶＰＮ」に関する説明においてＶＰＮ接続について触れました。若干イメージがつかみづらいかもしれませんので，その概要について，より詳しく御説明いたします。

そもそも「ＶＰＮ」とは，Virtual Private Network（バーチャル・プライベート・ネットワーク）の略でございまして，文字どおりネットワーク空間の中に仮想の専用ネットワークを構築することにより，先ほど御説明した通信内容を暗号化したものと比較して，より高いセキュリティを確保するための技術でございます。ＶＰＮ接続においては，仮想のトンネルを構築するトンネリング，暗号化，認証などによって，先ほど申し上げたような仮想の専用ネットワークを構築しております。

まず，トンネリングの御説明をいたします。トンネリングとは，ネットワークの中に拠

点間を結ぶ仮想のトンネルを構築し，外部から通信内容を盗み見られたり，その内容を改ざんされるといったことを防止するための技術でございます。スライド（８枚目）におきましては，「Ａ拠点」と「Ｂ拠点」との間をＶＰＮ接続によって結ぶ場合のイメージを示してございます。ＶＰＮ接続を行うためには，仮想の専用ネットワークを構築するためのＶＰＮ装置をデータの送信者と受信者の双方が備えている必要があるため，スライドにおける「Ａ拠点」・「Ｂ拠点」のいずれにもＶＰＮ装置が設けられております。ＶＰＮ装置と聞くと物理的な機器が念頭に浮かぶかもしれませんが，それだけではなく，一般的にテレワークで利用されているように，パソコンなどの端末にＶＰＮ接続のためのアプリケーションを入れることによってＶＰＮ装置の機能を果たすということが可能となってございます。その上で，先ほど申し上げたトンネリングについて，御覧いただいているスライドの中央に「ＶＰＮトンネル」と記載しているように，これらの拠点を結ぶネットワークの中にＶＰＮトンネルという仮想のトンネルを通すことにより，外部からの侵入を防ぐイメージであると御理解いただけるとよろしいかというふうに存じます。

次に，暗号化について御説明いたします。暗号化は，送信するデータをそのままでは判読することができない状態にするとともに，データを受信した者においては内容を判読することができる状態にすることによって，データの送受信の過程で外部からデータを見られたとしても，その内容を判読することができないようにする技術でございます。スライドにおいて説明いたしますと，「Ａ拠点」から「Ｂ拠点」にデータを送信する際，データの送信相手である「Ｂ拠点」以外の者が内容を判読することができないように，暗号化した上でデータを送信し，このデータを受信した「Ｂ拠点」において，暗号化されたデータの内容を復号化することにより，「Ｂ拠点」以外の者がデータの内容を判読することができないようにするということでございます。

最後に，認証について御説明いたします。通信相手の認証とは，データを送受信する相手が本人であることを確認するための技術です。これによって，ＶＰＮ接続によって通信をしようとする者が本人であることを確認し，それ以外の者との間で通信が行われないようにするということでございます。スライドにおいては，データを送受信しようとする「Ａ拠点」と「Ｂ拠点」との間で相互に通信相手が本人であることを認証して初めて，データを送受信することになります。

これまで御説明いたしましたように，セキュリティを確保しながら通信を行うためのサービスや回線には様々なものがございます。一般にいずれのサービスや回線を利用するか

は，利用者において，通信の利用場面や目的に応じて，それぞれのメリット・デメリットを踏まえた上で選択しているものと認識しております。なお，ここでは三通りしか御説明いたしませんでしたけれども，このほかにも様々な通信サービスや回線が活用されております。今後も技術の発展に伴って，更に様々な種類のサービスや回線が開発・活用されることも考えられます。刑事手続において，こうした通信サービスや回線を利用するに当たっては，利用することのできるサービスや回線のメリット・デメリットを踏まえた上で，目的に沿ったものを選択するというのではないかというふうに考えられます。

○小木曽座長　ありがとうございました。

それでは，先ほどと同じように，御質問・御意見を頂戴したいと思います。どなたからでも，お願いいたします。

○河津委員　御説明ありがとうございました。「専用回線」，「インターネットＶＰＮ」，「インターネット」の３種類の通信回線のセキュリティについて，理論上の違いがあることは理解いたしましたが，実際上の違いがどのような場面で現れるのか御説明いただけますでしょうか。

○進関係官　お尋ねの三つの通信サービスと通信回線のうち，インターネットＶＰＮ，それからＳＳＬ／ＴＬＳによるインターネットは，不特定多数の者が利用するインターネット回線を使用する点で専用回線と性質が異なっております。このうちＳＳＬ／ＴＬＳは，インターネット上でデータを送受信する際にデータの内容を暗号化する技術を用いることによってセキュリティレベルを高めるものです。インターネットＶＰＮは，このような暗号化に加えて，ネットワーク上の２点間を結ぶ仮想的な直結回線を構築する，すなわち，先ほど申し上げたトンネリングの技術を利用して，データの送受信者の間で言わば仮想のトンネルを構築することによって，通信のセキュリティレベルをより高めるものです。もっとも，セキュリティレベルを高めているとはいえ，インターネット回線を用いていることには変わりはございません。また，トンネルの出入口であるＶＰＮ接続の機器等が攻撃の対象となる場合もある点で，専用回線と比較するとセキュリティレベルが劣るということは否定できないというふうに考えられます。これらに対して，専用回線はインターネット回線を用いていないため，外部の他者によるアクセスの可能性が低く，飽くまで一般論ですが，最もセキュリティレベルが高いというふうに言えると考えます。

○河津委員　ありがとうございます。セキュリティの程度の実際上の違いについてもう少し具体的なイメージを持ちたいので，教えていただきたいのですが，例えばマイナンバーは

機密性の高い情報であるとされ，訴訟手続で提出する紙媒体の書類にもマイナンバーを不必要に記載しないことが求められています。他方で，社会一般においてマイナンバーを提供する必要のあるときは，しばしばインターネット回線を利用した送受信が行われていると思われます。専用回線やＶＰＮではなくインターネット回線を利用して通信したことが原因で，マイナンバー情報が第三者に取得されてしまうといった事態は実際にはどの程度生じているのでしょうか。あるいは，そのような事態は基本的にはデータの暗号化等の措置により防止されていると考えられるのでしょうか。

○進関係官　大きく二つあるというふうに考えられます。まず一つは，今お尋ねのマイナンバーに代表されるように，マイナンバー自身は特定個人情報でございますけれども，特定個人情報又は同様に機微な情報を扱うための措置として何が考えられているかということ，それから，二つ目はそういう特殊なものではなく，一般的にインターネットでやり取りされている情報というふうに区分されるというふうに考えられます。つまり，インターネットだからいろいろな情報を何も考えずに送られるかということになりますけれども，例えばクレジットカード情報のように，通常の情報と違って，入力するときに何らかの変換するような入力を用意するとか，それから，マイナンバーでよく用いられますのは，実際にはもうマイナンバーは送らないとか，そのように代替の入力手段というものを，特にマイナンバーに代表されるような機微な情報に対しては用いられるのが，これから重要になろうかというふうに考えられます。

したがって，情報の質によって，入力の方法も含めて，単に暗号化とかそういうものだけに期待するというか頼るのではなく，様々な入力手段，もっと言えば，入力しなくても分かるようにするとか，前もって別の手段で取っておいてひも付けするとか，いろいろな手段が考えられますので，一つ一つの情報としてどうするかというよりは，今後御検討いただく中で，どうしても機微な情報を扱う必要があるときには，何らかの方法で安全にそれを入手すること，その方法とは別な形で流通させるというようなことも御検討いただければよろしいのではないかというふうに考えます。

○小木曽座長　河津委員，よろしいでしょうか。

○河津委員　今の御説明は，インターネット回線を利用したことが原因で，そういった機密性の高い情報が直ちに漏えいする可能性が高いということは必ずしも言えず，どの回線を選択するかということとは別に，機密情報の取り扱い方について今後検討する必要があるということを御示唆いただいたという理解でよろしいでしょうか。

○進関係官　そうですね，ここに表がございますけれども（スライド７枚目），回線によるセキュリティということと，それぞれその回線やサービスを扱うために必要なデータの機微度によって使い方を変えるという両方の組合せで考えていただきたいということを申し上げました。

○佐久間委員　捜査・公判において非対面の方式により意思疎通を図る際に利用することができるような技術として，どのようなものがあるかについて，御教示いただけると幸いです。お願いします。

○進関係官　はい，分かりました。今の御質問，映像や音声の送受信というところだというふうに考えます。そのための基本的な技術として，今いろいろ話題になっておりますけれども，５Ｇのような通信インフラが整備されてきてございます。この５Ｇ，すなわち，第５世代移動通信システムでございますけれども，主な性能として，４Ｇ，第４世代と比較して，「超高速　１０倍から１００倍」，「超低遅延　大体１０分の１」，「多数同時接続１０倍から１００倍」といったようなものが備えられた通信システムでございます。現在広く利用されております第４世代，ＬＴＥというふうに呼んでおりますが，このＬＴＥと比較して，いずれの項目についても性能が格段に向上してございます。５Ｇによって，例えば解像度の高い動画を配信したり，遠隔地からの医療をより高い精度で行うことができたり，あらゆるものをインターネットに接続するためのＩｏＴをより一層使いやすくすることができると期待されております。

また，既に５Ｇの次の通信システムである「Beyond　５Ｇ」の導入が２０３０年頃には見込まれております。そのことを踏まえまして，例えば，総務省においては，令和２年１月から２０３０年代の社会において通信インフラに期待される事項や，その実現に向けた方向性等を検討する「Beyond　５Ｇ推進戦略懇談会」が開催されているようです。このように，５Ｇ，それからその次の「Beyond　５Ｇ」等，技術的にはどんどん高精度・高性能になっており，今後も，映像と音声を送受信する際に用いられる通信インフラは一層の発展が見込まれております。先ほど対面ということがございましたけれども，例えば，タイムラグによっては通信相手とのコミュニケーションに支障が生じるようなことはほとんどなくなっていくように思われます。

○佐久間委員　ありがとうございました。

○笹倉委員　過去の会合で海外にいる証人の証人尋問について意見を述べたことがありまして，その関係で，初歩的なことからもしれませんが，お尋ねします。ただいま，通信回線

のセキュリティを確保する技術について御説明いただきましたけれども，この御説明いただいた手段は，いずれも海外との間で情報をやり取りする場合にも基本的には使えて，通信が国内で完結する場合におけるのと同等程度のセキュリティが確保されると考えてよいでしょうか。それとも，海外との通信であるがゆえに考慮すべき事情があるでしょうか。

○進関係官　はい，分かりました。今の御質問，特に海外との通信ということだというふうに思います。海外との通信ということですと，通信事業者のサービスによるということになろうかというふうに思いますけれども，先ほどの表（スライド７枚目）の真ん中の「インターネットＶＰＮ」という点でございますと，インターネットがつながっているというところから，基本的には利用することが可能であろうというふうに考えます。また，一番左の「専用回線」のところに「広域イーサネットを含む」というふうに表現しておりまして，回線のところに「閉域網」と表現してございました。通信事業者によりましては，海外との間で閉域網を利用して通信するサービスを提供しているという事例もあるように聞いてございます。今後そういうサービスが増えてくるのではないかというふうにも考えられます。

○重松委員　先ほど，ＶＰＮ接続の説明の中で，通信相手の認証，すなわち，本人確認を経た上で通信が行われるというふうな御説明を頂きました。先ほど来，映像や音声の送受信についてのお話が続いておりますけれども，例えば，ビデオリンク方式による取調べや，あるいは接見交通，そういった場面を想定したときに，なりすましとか，あるいは第三者の不当な介在，こういったものを防止するための技術的な措置としてはどういうものがあるのか，もしあれば御教示を頂きたいというふうに思います。

○進関係官　はい，分かりました。まず，先ほどＶＰＮの説明の中で本人確認という表現をいたしましたけれども，その部分の本人確認というのは，飽くまでも通信の相手先ということでの確認でございます。ですから，今の御質問でいう，いわゆる本人性の確認というところは，また別の話になろうかというふうに思いますので，分けて御説明いたしたいというふうに思います。

まずは，インターネットＶＰＮの御説明の中でお話しいたしました本人確認というのは，本人の接続先という点での確認です。ですから，本人性というのとはちょっと違います。今回の御質問は，正に本人性の確認というふうに承って，お答えいたします。

まず，身近な例としましては，本人にＩＤを割り当てて，本人がパスワードを設定することにより，このＩＤとパスワードで本人確認を行う方法が考えられます。また，二段階

認証等とも組み合わせるというようなことも一般的に用いられておりまして，導入が容易であるという点がメリットではなかろうかと考えます。他方，デメリットとしては，ＩＤやパスワードが第三者に知られてしまうと容易に本人以外の者がログインすることができてしまうということが挙げられます。

次に，映像と音声によって通話相手の容貌を確認する，必要に応じて身分証など本人確認書類を提示してもらうことにより本人確認を行う方法が考えられます。映像と音声によって通話をすること自体は一般的に行われているということから，通信環境を整備すれば直ちにこのような本人確認を行うことができるのがメリットでございます。他方，デメリットとしては，画像解像度が低ければ，通話相手の容貌を映した画像によって本人かどうかを判別することが難しく，また，本人確認書類の偽造などを発見することも容易ではなかろうという点が挙げられます。

また，先ほどマイナンバーという話が出てきましたけれども，例えばマイナンバーカードをカードリーダーで読み取らせ，暗証番号を入力させることにより本人確認を行う方法も考えられます。マイナンバーカードを利用して本人確認を行うため，遠隔地からであっても十分に本人確認を行うことができるのがメリットであろうと考えられます。他方，デメリットとしては，当然のことですが，マイナンバーカードを取得していない者について，このような方法により本人確認を行うことはできないという点になります。

また，指紋や静脈などを登録済みのデータと照合して本人確認を行う方法も考えられます。これらは身体的特徴ですから，各人に固有のものであるので，偽造することは容易ではなく，十分に本人確認を行うことができるのがメリットですが，デメリットとしては，本人確認に当たってデータを照合するために，あらかじめ本人確認を求めようとする者の指紋や静脈などをデータとして取得して，それを保管しておかなければならないという点が挙げられます。

このように，現時点でも様々な方法がございますので，それをどのように組み合わせるかということが検討の対象になろうかというふうに考えられます。

○小木曽座長　ありがとうございます。

ほかはいかがでしょうか。御質問なければ，御意見でも結構です。

○池田委員　「通信サービス・回線の技術及び安全性」に関して，ただいま進関係官からの御説明を伺いまして，セキュリティを確保しながら通信を行うための通信サービスや通信回線としては様々な種類のものがあって，利用者はその中から通信の利用目的や場面に応

じてそれぞれのメリット・デメリットを踏まえた上で，ニーズに沿うものを選択しているのが実情であるということについて理解いたしました。

刑事手続との関係で考えますと，そこで取り扱われる情報の性質に照らせば，通信のセキュリティを確保することが重要であるということになりますので，そのことを踏まえた上で適切な通信サービスや通信回線を選択するのであれば，オンラインによって刑事手続を行うこととすること自体は現実的なものとして考えられるように思われます。

また，進関係官からは５Ｇや「Beyond　５Ｇ」についても御説明を頂いたところですが，情報通信技術が著しく発展している現在と比較しても想像がつかないような通信環境が整備される世界が訪れ得るということでありまして，リアルタイムで高精細な映像によってコミュニケーションを図ったり，大容量のデータを瞬時に送受信したりすることも大いに期待できる状況にあるということが改めて理解できました。これを踏まえますと，現在の議論を反映した形で刑事手続法の改正が行われまして，それが施行される時期には，技術的には刑事手続においても様々な場面でオンラインを活用することも期待できるものと考えられます。

冒頭で申し上げたとおり，いずれの手続にどのような通信手段を用いるかは，それぞれの特徴を踏まえて技術的観点から今後検討がされるべきものと思われますし，また，回線のセキュリティのみならず，その他の技術も組み合わせて，全体としてセキュリティを考えることが重要であるという御指摘も頂いておりますけれども，いずれにしても，本検討会においてはこうした技術的な発展も見据えた上で法的課題についての検討を進めていくこととしてよいのではないかと考えております。

○河津委員　今日の社会では，一定の機密性を有する情報についても，通信データを暗号化した上でインターネット回線を利用した送受信が一般的に行われていると理解しております。このような通信の方法は，機密情報を記載した紙媒体を物理的に運搬する方法と比較しても，一概にセキュリティリスクが大きいとはいえないと思われます。また，今後セキュリティを確保するための技術は更に進歩することが期待されます。もちろん電子データの特性を考慮する必要はありますし，進関係官からも御示唆があったとおり，情報の機密性の程度に応じた措置を講じることにより合理的な水準のセキュリティを確保する必要があることは間違いありません。ただ，その議論に当たっては，インターネット回線を利用する点を過度に評価して，官公庁の外部にいるためインターネット回線を利用せざるを得ない国民・市民の権利利益が損ねられることのないよう，留意する必要があると考えます。

○小木曽座長　ありがとうございました。

ほかに御意見，よろしいでしょうか。

特になければ，一通り御意見を頂戴できたと思いますので，「通信サービス・回線の技術及び安全性」についての意見交換はこの辺りで一区切りといたしたいと思います。

次のテーマに移ります前に，１０分程度休憩を取りたいと思います。

（休　　憩）

○小木曽座長　では，ここからは「３　電子データの改ざん防止措置」についての御説明をお願いしたいと思います。

進関係官，よろしくお願いいたします。

○進関係官　それでは，「電子データの改ざん防止措置」について御説明いたします。

本検討会においては，従来紙媒体で作成・管理されたり，紙媒体で発受されてきた書類について，これを電子データとして作成・管理することができるようにし，電子データとしてオンラインにより発受を行うことができるようにするという議論がなされているところでございます。一般に電子データは紙媒体に比べて改ざんの痕跡が残りづらく，故意又は過失によって電子データの内容が書き換えられても，これに気付くことが難しいという性質を有しているため，電子データの作成者を明らかにするとともに改ざんを防止するための技術が開発されております。そこで，本検討会での議論に資するよう，電子データの非改ざん性を担保する技術的措置について，検討会でも触れられていた電子署名という技術のほか，タイムスタンプという技術を中心に，その概要を説明いたします。

まず，電子署名について，スライドを使ってその仕組みを説明いたします。電子署名とは，電子データに記録された情報について，その作成者が誰であるかを示すとともに，電子データの内容等が改変されていないかどうかを確認することができる措置です。電子署名には暗号化の技術が用いられており，ここでは一般的に用いられている公開鍵暗号化方式という電子署名の仕組みについて，その概要を簡単に説明いたします。

今までの内容と比べて少しややこしいので，少しアニメーションを使って御説明いたします。このスライド（スライド１０枚目）では，電子データを作成し，電子署名を利用する者を「作成者Ａ」，Ａが作成した電子データを受信する者を「受信者Ｂ」としております。

まず，電子署名を付すために必要となる鍵等について御説明いたします。作成者Ａは，電子署名を利用するための鍵，具体的には秘密鍵と公開鍵を入手する必要がございます。秘密鍵と公開鍵を入手する方法は幾つかあるところ，ここでは第三者機関である認証局から電子証明書と共に発行を受けて入手する方法を前提に御説明いたします。

Ａはスライドの「①」で，認証局に対して電子証明書，秘密鍵及び公開鍵を発行してくれるよう申請を行います。スライドの「②」で，認証局から電子証明書，秘密鍵及び公開鍵の発行を受けます。このうち秘密鍵は，印鑑でいうところの実印に相当するものであり，本人が厳重に管理すべきものであって，本人以外の人が他人の秘密鍵を使うことはできないということになってございます。他方，公開鍵は秘密鍵とペアになるものであり，電子データのやり取りを行う相手方に渡すことが予定されているものでございます。公開鍵は認証局から発行される電子証明書に格納されており，言わば電子証明書は印鑑でいうところの印鑑登録証明書に相当すると考えられます。秘密鍵で暗号化したデータについては，ペアとなる公開鍵でしか開けることができません。公開鍵暗号化方式による電子署名は，こうした秘密鍵・公開鍵の機能を利用することで，誰が文書などの電子データを作成したかを確認できるようにするものでございます。

次に，電子署名を付す場面について御説明いたします。作成者Ａは，自分が作成した文書などのデータについてハッシュ値を得ます。ハッシュ値とは，電子データに記録された数値や文字列のデータをハッシュ関数という一定の計算式を使って演算し，一定の長さに変換した文字列です。同じハッシュ関数を使えば，元の電子データの大きさに関係なく，常に同じサイズのハッシュ値が得られます。ハッシュ値は通常，元の電子データに比べてデータのサイズが小さいため，簡単に取り扱うことができます。ハッシュ値の特性上，同じハッシュ関数を用いたとしても，基となる電子データの内容が少しでも違うと全く異なる値が得られることになります。電子署名は，このようなハッシュ値の特性を利用することで，電子データの内容に改変がないかを確認できるようにするものです。

そして，作成者Ａはスライドの「③」で，このハッシュ値を自分の秘密鍵を使って暗号化し，電子署名を作成いたします。電子署名とは，この秘密鍵によりハッシュ値を暗号化したデータのことです。このようにしてＡは電子署名を作成した後，スライドの「④」，「送信」と書いてございますが，ここで電子データ，電子署名，電子証明書をセットで受信者Ｂに送信いたします。

次に，受信者側で電子署名を検証する場面について御説明いたします。受信者Ｂは，Ａ

から送信された電子データがＡが作成したものであるかや，Ａが作成して以降，改変されていないかを確認いたします。そのためにＢは，まずスライドの「⑤」で，受信した電子証明書について，これを発行した認証局に対して，この電子証明書が作成者Ａの有効な電子証明書であるかを確認いたします。そして，これが有効であることが確認できた後，スライドの「⑥」で，その電子証明書に格納された公開鍵を使ってＡから送られてきた電子署名の暗号を復号し，元のハッシュ値を得ます。このようにして，作成者Ａの有効な電子証明書に格納された公開鍵によって電子署名が復号化できたということは，これがペアとなる作成者Ａの秘密鍵で暗号化されたことにほかならないことから，この電子署名が，いわゆるハッシュ値のところですが，作成者Ａによって作成されたことが確認できることとなります。

さらに，Ｂは電子署名を復号化して元のハッシュ値を得るだけでなく，自らもＡから受信した電子データ自体から，作成者Ａが用いたものと同じハッシュ関数を使って演算し，ハッシュ値を得ることができます。そして，Ｂは，こうして得られた二つのハッシュ値を比較し，これが一致するかどうかを確認いたします。先ほども述べましたとおり，電子データの内容が一部でも変更されていれば，同じハッシュ関数を用いたとしても得られるハッシュ値が異なるものとなるため，二つのハッシュ値が一致した場合は，受信したデータの内容は作成者Ａが電子署名を作成したときから改変されていないことが確認できることとなります。他方，二つのハッシュ値が一致しない場合，受信した電子データの内容は，作成者Ａが電子署名を作成したときのものから改変されている可能性があるということになります。

少し混雑した絵でございますけれども，数字の番号どおりたどっていただければ電子署名の仕組みについてお分かりいただけると思います。以上が電子署名の仕組みの御説明でございました。

次に，タイムスタンプについて御説明いたします。タイムスタンプとは，対象となる電子データから得られたハッシュ値と時刻情報がセットになったものであり，タイムスタンプに記録されている時刻に当該電子データが存在していたこと，その時刻以降にその電子データの内容が改変されていないことを証明するための措置です。一般にタイムスタンプは郵便局の消印，通信日消印ですね，と同様の機能を有するとされております。ここでもアニメーションで御説明いたします。スライド（１１枚目）では，電子データを作成し，今度はタイムスタンプを利用する者を「利用者Ａ」，Ａが作成した電子データを受信する

者を「受信者Ｂ」としてございます。

まず，タイムスタンプを発行してもらう場面について御説明いたします。利用者Ａはスライドの「①」で電子データを作成し，そのデータについてハッシュ関数を使って演算してハッシュ値を得ます。そして，Ａはスライドの「②」でこのハッシュ値を時刻認証局に送り，タイムスタンプを発行するよう要求いたします。時刻認証局はＡの要求を受けて，Ａから送られたハッシュ値と時刻情報をセットにしたタイムスタンプを作成し，スライドの「③」で，これをＡに発行いたします。ここにございます時刻情報は日本標準時に基づいた正確な時刻であり，正確性が担保されてございます。なお，ハッシュ値から元の電子データの内容を再現することはできませんので，時刻認証局が受け取ったハッシュ値からＡが作成した電子データを再現し，その内容を見ることはできないことになります。そして，スライドの「④」で送信というところがございますが，利用者Ａは電子データと発行されたタイムスタンプをセットで受信者Ｂに送信いたします。

次に，タイムスタンプにより検証を行う場面について御説明いたします。受信者Ｂはスライドの「⑤」で，受信したタイムスタンプが有効であるかどうかを時刻認証局に確認し，有効であることが確認できた後，受信した電子データについてＡが用いたものと同じハッシュ関数を使って演算し，ハッシュ値を得ます。そして，Ｂは電子データから得られたハッシュ値とタイムスタンプに格納されているハッシュ値を比較し，これが一致するかどうかを確認いたします。二つのハッシュ値が一致する場合，タイムスタンプに組み込まれた時刻情報の日時に当該電子データが存在し，その後にその内容が改変されていないことが確認できることになります。他方，二つのハッシュ値が一致しない場合，タイムスタンプに組み込まれた時刻情報の日時に当該電子データが存在したことが確認できない，すなわちタイムスタンプが施された後にその内容が改変された可能性があることとなります。

なお，電子署名にもタイムスタンプと同様，電子署名が施された以降，電子データの内容が改変されていないことを確認する機能はございます。ただ，電子署名が施された時刻として記録される日時は電子署名を行った端末，ＰＣ等になりますが，その設定時刻にすぎないので，端末の設定時刻が正確な日時からずれておりますと，そのずれた時刻が記録されることになってしまいます。これに対してタイムスタンプの場合，タイムスタンプに記録される時刻は第三者である時刻認証局が日本標準時間に基づいて発行するものであるため，タイムスタンプが施された電子データが存在した正確な日時が記録され，これを証明することが可能になります。このようなことから，タイムスタンプは電子データが存在

した正確な日時を記録しておくために用いられるものでございます。

以上がタイムスタンプの仕組みについての御説明でございました。

○小木曽座長　ありがとうございました。

それでは，先ほどと同じように御質問・御意見を頂戴いたしたいと思います。お願いします。

○重松委員　先ほどの御説明の中で，電子署名の認証局，あるいはタイムスタンプの時刻認証局という言葉が出てまいりましたけれども，こういった認証局や時刻認証局としては，現状どのような機関が存在しているのでしょうか。また，その中に公的な機関はあるのでしょうか。よろしくお願いします。

○進関係官　まず，認証局でございますけれども，政府認証基盤，これはＧＰＫＩというふうに申し上げますけれども，このＧＰＫＩにおける政府共用認証局が存在しております。例えば，裁判官・検察官・警察官といった公務員につきましては，この政府共用認証局を利用して電子署名を付すことが考えられます。また，電子署名自体は広く一般に社会の中で利用されておりまして，政府が認定したものも含め，利用可能な認証局が複数存在しておりますので，公務員以外の方につきましてはこれらの認証局を利用することができます。他方，タイムスタンプにつきましては現在のところ政府の認証基盤は存在してございません。いずれにいたしましても，仮に刑事手続においてこのような電子署名・タイムスタンプを利用するということですと，その時点における認証サービスの状況を踏まえて御検討いただければというふうに考えてございます。

○河津委員　電子署名の秘密鍵について，本人以外は使えないものであるとの御説明を頂きましたが，本人以外が秘密鍵を使うことができないことを担保する方策としてどのようなものが考えられるのか，御説明いただけますでしょうか。

○進関係官　まず，本人が使うものと言いましたものは，その前提で作られているということでございます。ですから，委員御指摘のように，第三者が悪用しないことを担保するために何らかの方策を取る必要がございます。申し上げたように，一般に，秘密鍵は厳重に保管・管理することが求められております。

例えば，秘密鍵を利用する方のＩＤカードの中に秘密鍵を格納して保管・管理するといったように，パソコン端末の中に入れないというような方策がございます。使用する場合にはＩＤカードをカードリーダー等で読み取った上で専用のパスワードを入力するというような仕組みが考えられます。このような仕組みにしておきますと，秘密鍵がＩＤカード

の中に格納されますので，例えば，通信回線を通じて盗まれるリスクとか，そういうことを回避することができますし，仮にＩＤカードが盗まれてもパスワードで読み出すので，パスワードが分からなければ電子署名を使用することができないというようなことがございます。

ただ，飽くまでも何らかの形で保存することになりますので，御指摘のように，保管・管理が不十分で，例えば盗まれるとか，無くなるとかいったようなことも考えられます。そのような場合には，ＩＤカードが無くなったことに気付いた時点で，秘密鍵を無効化することを先ほどの認証局に申請することによって，この秘密鍵はもう無効になっているよということが分かるようにすると，そのことによって第三者に悪用されることを防止するというようなことができるようになってございます。

○佐久間委員　電子データの改ざん防止措置について，２点御教示いただきたい点がございます。

まず１点目は，電子署名・タイムスタンプを付した後の訂正・追記についての質問です。現在の実務においては，書類を紙媒体で作成し，署名押印後に訂正すべき記載を発見した場合には，刑訴規則５９条に従って，手書きで訂正した上で訂正した部分に認印，いわゆる訂正印を押すといった取扱いがされておりますが，電子署名やタイムスタンプを付した電子データについて訂正の必要が生じた場合には，どのような措置を講ずることが考えられるのでしょうか。また，刑事手続において作成する書類の中には，令状など，一つの書面に複数の作成者が署名押印を行うものがあるのですが，電子署名やタイムスタンプを付した電子データについて内容を追記する必要が生じた場合には，どのような措置を講じることが考えられるでしょうか。

２点目は，電子署名の有効期間に関する質問でございます。刑事手続においては，刑事確定訴訟記録など，事件記録を長期間にわたって保存することが必要となります。このような長期保存が必要な電子データについて，有効期間が設けられている電子署名を用いることとして不都合は生じないのでしょうか。

以上２点について御教示いただけると幸いでございます。よろしくお願いします。

○進関係官　それでは，１点目の追記や訂正について御説明いたします。

御指摘のように，電子署名やタイムスタンプを施した電子データの内容そのものを直接変えてしまいますと，ハッシュ値が変わってしまいますので，事後に一致を確認することができなくなってしまうことから，もともとの確認ができないということになってしまい

ます。そこで，訂正や追記のための仕組みが幾つかございます。ここでは二通り御説明いたします。

まず，一通り目は，元の電子データに追記した内容を記録した電子データ，例えばコメントですとか，先ほど，令状のように追記そのもの，別の追記があるというふうに御説明がありましたけれども，そのようなものを添付して，それら電子データの全体に，追記した者が新たに電子署名を施す方法がございます。つまり，今までのデータの外に追記変更した部分を作って，そして，今までのものとを含めて全体に対して電子署名を施すという形でございます。

それから，二つ目でございます。元の電子データを複製した電子データに訂正や追記を施して，新たな電子データを作成して，この新たな電子データを元の電子データと共に一つのファイル，例えば圧縮等が考えられますが，そのまとめた上で，そのファイル全体に訂正追記した者が電子署名を施す方法がございます。これは，先ほどの追記に比べまして，第１版と第２版を合わせて，その二つに署名を施すといったような形でございます。これが，御指摘の１点目の御説明でございます。

２点目の有効期間についての御説明をいたします。御指摘のように，電子署名には有効期間がございます。電子署名は，秘密鍵を用いて電子データから得られたハッシュ値を暗号化して作成するものでございます。暗号化の技術は，技術の進展に伴って破られるリスクが高まるので，電子署名についても署名を施した後に時刻が経過するにつれて暗号が破られるリスクが高まります。このようなリスクを考慮しまして，電子署名に用いられる電子証明書には，法令上，５年を超えないものという有効期間が設けられてございます。したがって，現在，発行される電子証明書には，最長で５年の有効期間が定められており，その期間を超えると失効いたします。これを受信した者は電子証明書が有効であることを確認できませんので，電子署名を検証できないということになります。

そこで，有効期間が経過した後に電子署名を検証することを可能にするために，先ほどタイムスタンプの御説明をいたしましたが，電子署名にタイムスタンプを組み合わせた長期署名という技術がございます。長期署名では，対象となる電子データ，電子署名，それから当該電子署名の電子証明書，それから失効情報，そういうグループのデータ全体に新たにタイムスタンプを付与します。これにより，電子署名や検証に必要な情報等がタイムスタンプの暗号アルゴリズムで保護されます。実はタイムスタンプの暗号アルゴリズムは，個人の電子署名に用いられるものよりも強固です。そのため，タイムスタンプの有効期限

は１０年とされてございます。このような形でタイムスタンプを併用するということで新たに期間，期限を延ばすということが可能になりますし，同じことを更に次の期限の手前でやれば，もう１０年延びるということで，組み合わせて使っていただくというようなことが考えられます。

○佐久間委員　ありがとうございました。

○重松委員　電子署名については，あらかじめ認証局から電子証明書の発行を受けておく必要があるとの御説明でありましたけれども，一般の方が平素からそのような電子証明書を持っているということはなかなか想定し難いことかなというふうに考えております。この点，例えば供述調書の作成に当たって，供述者が電子証明書を持っていない場合に，現行の署名押印に代わる措置として，電子署名以外にどのような技術的な措置が考えられるのでしょうか。御教示いただければと思います。

○進関係官　御指摘のように，電子署名に必要な鍵を入手していないということから直ちに電子署名を利用することが難しい方がいらっしゃるという想定につきましては，いろいろな方法が考えられるというふうに思います。今，御指摘いただいた署名や押印というところで考えますと，現行の署名に代わるものとしましては，例えば，クレジットカードを利用したときに書くようなタブレットがございますが，タブレット端末の画面にタッチペンで氏名を手書きするような方法，それから，押印につきましては，現在でも指印が利用されているというふうに承知してございますが，指紋を画像データとして採取して，その画像データを作成された電子データに貼り付けるといったような方法が考えられます。

もちろん，このような方法には，氏名を手書きした後に当該電子データの内容が改変されていないことを担保する機能はございません。そのため，更に非改ざん性を担保したい場合にどのようなことが考えられるかということですけれども，例えば，電子署名を行うことができる別の者が，先ほどの署名に代わるタッチペンですとか，押印・指印に代わる指紋データですとか，そのような電子データに対して電子署名やタイムスタンプを施すというようなことが考えられるのではないかというふうに思います。

指紋ということになりますと，後に使い回すというような議論も懸念されるのではないかというふうに考えますけれども，先ほどの電子データという点で言えば，電子データに指紋のデータを貼り付けたときに，ファイナライズというような表現がございますが，そのデータを固定するというような意味でございますが，ほかに使えないようにすることも技術的には可能ですので，そのような技術をどのように活用されるかということを検討い

ただいて，いろいろな技術を活用いただければというふうに考えます。

○重松委員　続けて質問させていただきます。警察の捜査実務におきましては，例えば，事件が発生しますと現場に急行して，付近の目撃者の方からお話を聞いて，場合によってはその場で供述調書を作成するとか，あるいは，例えば交通違反の取締りに際しても，交通違反切符の作成に際して，違反者から供述者欄に署名押印を求めるというふうなことがございます。このように，警察施設以外の外において様々な活動がありまして，その過程において様々な書類を作成することがあるのですが，例えば，電子署名あるいはタイムスタンプ，あるいは，先ほど御説明のあったタッチペン等々を屋外で利用するという場合には，どういった機器あるいは環境が必要となるのか，教えていただければと思います。

○進関係官　今，御指摘いただいたように，電子署名を施す者が電子署名の利用に必要となる秘密鍵を自らのＩＤカード等に格納して保管・管理するという場合，外出先ではカードリーダーが必要となるというふうに考えます。ですから，パソコン端末等と接続できるようなカードリーダーがやはり機器として必要になろうかというふうに考えられます。また，タイムスタンプの場合には，先ほどアニメーションで御説明いたしましたが，時刻認証局からタイムスタンプの発行を受ける必要がございますので，通信のための通信環境・通信機器が必要になるというふうに考えられます。また，先ほどの署名や指紋という点ですと，例えばタッチペンが使える端末，そのような機器の準備がやはり必要になろうかというふうに考えられます。

○永渕委員　ただいま電子データの改ざん防止の措置として，電子署名やタイムスタンプというものを御紹介いただいたわけですけれども，これらの技術的措置以外に，改ざん防止のための手段として何か技術的な措置の例があるようであれば，御教示いただけると幸いです。よろしくお願いいたします。

○進関係官　先ほどは，認証局ですとか時刻認証局を用いた電子署名やタイムスタンプについて御説明いたしました。その他の電子データの改ざん防止の措置として考えられますのは，例えばということでございますが，電子データを保存するサーバの中に特定の領域を作って，その特定の領域に保存した場合に内容を改変することができなくなるような仕組みをシステムとして構築するというような措置が考えられるのではないかというふうに思います。これらのような仕組みは，電子署名やタイムスタンプとは異なりまして，認証局や電子証明書は不要でございます。その領域に保存することができる人は誰でも利用することができるというようなメリットはございます。

しかし，他方，電子署名のように本人しか使うことができないような秘密鍵というようなものではないので，例えば，システムのアクセス権限とか履歴によるかもしれませんけれども，誰が作成者であるかが必ずしも分からないという点でございましたり，また，その領域から一旦出てしまうと改変の担保は及ばないので，そのような場合にどのようにそのデータの非改ざん性をどう担保するかという点などにつきまして，また別の課題として検討すべきというふうに思っております。

一例でございました。

○永渕委員　ありがとうございました。

○小木曽座長　ほかに御質問はございますか。なければ御意見でも結構ですが，お願いいたします。

○笹倉委員　署名押印等について，ただいまの進関係官の御説明を受けて，意見を述べたいと思います。

私は，過去の会合で，署名押印あるいは契印等に代わるものとしてどのような措置を必要とすべきかについて，署名押印等が求められる趣旨等を踏まえて検討する必要があるという意見を述べたところです。その趣旨としては，書類の作成・記載の真正を担保するにあると考えられますところ，本日，進関係官から御説明いただいたところによれば，電子署名という技術があり，それによって電子データの作成者が誰であるかという作成の真正を担保する機能や，電子署名が施された後に当該電子データの内容が改変されていないという内容の非改ざん性を担保する機能があるということでございましたし，さらに，タイムスタンプという機能によって電子署名が付された正確な日時を証明することで，その署名の機能が補完されるということでもございました。

このような技術があるのだとしますと，それは，現行法上，署名押印等が要求されている趣旨を満たしていると言ってよいように思われます。もちろんその要求を満たすためには，ただいま御議論がありましたように，設備が必要であるとか，装置が必要であるとか，そういったいろいろな問題はあるでしょうし，また，更に今後優れた技術が開発されるということがあるかもしれませんが，現時点の技術水準でも，現行法上，物理的に紙に署名をするとか押印をするとかいうことが要求されている趣旨を満たしつつ，それに代わる技術的措置を講じることは可能であると理解しました。

今後はそのことを踏まえた上で，書類を電子データとして作成できるようにするための方策について，この場で検討していくことが適当であると考えます。

○池田委員　私からも，署名押印に代わる措置について意見を申し上げます。現在の署名押印を電子署名で置き換えることとする場合，身体の拘束を受けている被疑者などのように，直ちに電子署名を利用することが難しいという者もいることに鑑みますと，例えば，供述を録取した供述調書を電子データとして作成した場合に，これに供述者として署名又は押印をするように求めるとして，どのような措置を取るべきかを検討する必要がありますけれども，そのためには，現状で供述録取書に録取された供述を証拠として用いるための要件として，供述者の署名押印が求められている趣旨等を踏まえておく必要があるように思います。

供述録取書は，その作成に当たり，供述者の供述を録取者が聴き取って，その内容を記憶して，文章の形に構成して書面に記載する，そういう過程を経るために，聞き取り，記憶，文章構成，そして記述というそれぞれの過程で誤りが生じるおそれがあって，ひいては録取書の内容が実際になされた供述を正確に反映しないものとなるおそれがあるとされており，不正確に書面に録取された供述は，これを証拠とすることができませんが，このときに供述者自身が記載内容を確認した上で署名押印したものであれば，実際にそこに書かれている供述をしたこと自体は確かであると言えることになります。

このように，録取が正確にされたことを供述者本人が担保することに供述者の署名押印を求める趣旨があるということになりますと，こうした趣旨との関係では，本日御紹介があったような，タブレット端末の画面にタッチペンでサインを手書きするという技術的措置や，指紋を画像データとして採取して貼り付けるという技術的措置を用いることによっても，供述者が供述調書の内容を確認して，自らの供述が正確に録取されたことを承認したことを表すものとして扱うことは可能であると考えられます。

もちろん，今後，更に優れた技術が開発されるかもしれませんけれども，現時点での技術水準でも，供述者の署名押印に相当する技術的措置を講じることは可能であるものと考えられます。

なお，このような技術的措置そのものには供述調書たる電子データの内容の非改ざん性を担保する機能はないという御指摘がありましたけれども，供述者が署名押印に相当する技術的措置を施した後で，取調べを行った捜査官等が当該措置を含む供述調書たる電子データの全体について電子署名等を施すこととすれば，電子データ全体について，その改ざん性を担保することができるという御指摘も頂いており，そのような対応を取ることが考えられます。

○小木曽座長　ありがとうございます。

ほかに御質問・御意見はよろしいでしょうか。

では，一通り御意見を頂いたと思いますので，「３」の「電子データの改ざん防止措置」についての意見交換はこの辺りで一区切りといたしたいと思います。

最後に，「４　その他」としまして，これまでの「１」から「３」までのテーマ以外の事柄につきまして御質問・御意見がありましたら，お願いいたします。

吉澤委員，どうぞ。

○吉澤委員　ＩＴ化に際して気を付けなくてはいけないことの一つとして，障害者への配慮というものもあると思います。被害者御本人が障害をお持ちの場合もありますし，例えば，被害に遭われたことで障害が残るというケースもあります。また，被害者の代理人となる弁護士が障害を持っているケースもありますので，そういう障害のある当事者や代理人にとっても，できる限り刑事手続を使いやすい形にするということを常に考える必要があると思っております。

例えば，視覚障害のある方にとっては，紙ベースの書類の内容を確認することについて，現在でも，音声読み上げソフトなどを駆使するなどして非常に苦労されている，そのようにしながら対応されていると思うのですが，今回，先ほどの書類の電子データ化の話もありましたが，そのように書類を電子データ化する際，例えばどのような形式でデータ化してもよいというふうにしてしまうと，結局，障害者にとっては非常に使いにくいとか，場合によっては様々な形式の電子データへの対応が必要となるなどという理由で，より使いにくくなるということも考えられます。

そこで，書類について電子データ化する際，どういったことに配慮し，どういった方式や形式を取れば障害のある方にとっても利用しやすいというふうになるのか，具体例などありましたら御教示いただければと思います。お願いします。

○進関係官　先ほど音声読み上げソフトというような御説明がございましたけれども，最近のＰＣ又はＯＳ等では多様性に配慮したいろいろなインターフェースが用意されてございます。ですから，基本的に従来の紙ベースのものに対しては，例えば，これを読み上げるソフトがありますが，現状の音声読み上げソフトは恐らくテキスト化されたデータを読み上げるというものであろうというふうに思います。最近のものですと，ＡＩ　ＯＣＲというようなものがございまして，ＯＣＲというのは光で文字を読み取るもの，そして，それにＡＩが組み合わさっているので，文字を読み取って，ＡＩがそれをよりしっかり読み取る

と，その読み取り精度も格段に上がっているということもございますので，いろいろ書かれたものも，テキストとして入力されていなくても，いろいろ読み上げられるというような機能もございます。また，視覚ですとか聴覚ですとか，そういういろいろな障害をお持ちの方に対して，いろいろなＯＳのインターフェースでそれをサポートする，又は，逆にその障害者の方が御希望になるインターフェースに合わせて変換してお出しするというようなこともどんどん進歩してくるのではないかというふうに思っております。

ですから，一つはいろいろなメニューを用意しておくこと，それから，更に御希望のメニューに対して対応していくことができるように，更にメニューを増やしていくというようなことが考えられますし，それから，単にメニューだけではなく，先ほどＡＩというようなお話もしましたけれども，より分かりやすく御説明するとか，そういうようなことも考えられていくのではないかというふうに思っております。

なかなか具体例という点では，今のＯＳが様々な対応を開始しているとか，そういうことしか今は御説明できませんけれども，技術的にはよりいろいろな方に優しいインターフェースということで開発が進んでいるというふうに承知しております。

○成瀬委員　進関係官に質問させていただきたいと思います。今後，刑事手続において情報通信技術を活用していく中で，システム障害や大規模停電などが生じることも考えられますが，それらに対して，どのような対応策が考えられるのでしょうか。御教示いただければ幸いです。

○進関係官　御指摘のようなことは具体的なシステムという点ではなかなか御回答しにくいので，一般論として申し上げさせていただきます。

システム障害への備えとしては，例えばバックアップデータを持つとか，いろいろなバックアップのサーバを利用するとかいうことが考えられます。これによって，通常的に使用している機器ですとか回線ですとかに障害が生じた場合でも，予備の機器とか予備の回線を利用することで，障害の影響を受けずに継続することができるのではないかと思われます。また，停電への備えとしては，非常用の発電設備でございますとか，そのようなことをやはり準備する必要があろうかというふうに思っております。さらには，機器等も消費電力が少なくなってございますので，従来よりも非常用発電設備が小さくて済むとか，少なくて済むというようなことも，今後，進んでいくのではないかというふうに考えられます。

○小木曽座長　ありがとうございます。

ほかはいかがでしょうか。よろしいですか。

それでは，一通り御意見を頂戴したと思いますので，「その他」につきましてもこれで一区切りといたしたいと思います。

本日予定しておりました議事は以上であります。

進関係官には大変分かりやすい御説明をいただき，ありがとうございました。御礼申し上げます。

それでは，次回以降の検討の進め方ですけれども，前回会議までに論点項目の各論点につきまして一巡目の議論を終えております。今後は二巡目の議論に入っていくことにしたいと思いますが，次回会議におきましては，論点項目の「１　書類の電子データ化，発受のオンライン化」の各論点，すなわち（１）書類の作成・発受，（２）令状の請求・発付・執行，（３）電子データの証拠収集，（４）閲覧・謄写・交付，（５）公判廷における証拠調べ，この五つの論点について，一巡目の議論を踏まえて，焦点を絞って議論をしたいと考えております。そのような進め方でよろしいでしょうか。

（一同了承）

ありがとうございます。

本日の会議の議事につきましては，特に公表に適さない内容はなかったと思いますので，発言者名を明らかにした議事録を公表いたします。また，進関係官からの説明資料につきましても公表することにいたしたいと思います。そのようなことでよろしいでしょうか。

（一同了承）

では，そのようにいたします。

次回の予定につきまして，事務当局から説明をお願いします。

○仲戸川室長　次回の第６回会議でございますが，９月中旬頃の開催を予定しております。本日まで日程が決まらず，御迷惑をお掛けいたしますが，現在，最終の日程調整中でございます。確定し次第，皆様にお知らせをいたします。

次回の会議も本日と同様にウェブ会議方式で実施する予定でございます。どうぞよろしくお願いいたします。

○小木曽座長　本日はこれにて閉会です。

どうもありがとうございました。

－了－