i-TECセミナー

持出PCのセキュリティ
ー情報漏洩の現状および対策技術についてー

2019年10月18日

才所敏明
(株)IT企画・代表取締役社長
toshiaki.saisho@advanced-it.co.jp
http://www.advanced-it.co.jp
https://www.facebook.com/toshiaki.saisho

自己紹介

1966年　東京大学入学(工学部・計数工学科・数理コース卒)

1970年　東芝入社

社内計算機利用環境企画・構築・活用指導・支援

スーパコン～PCを利用した技術開発環境構築・活用推進(1969UNIX)

インターネットの企業活動への活用推進

(1974Internet　1984JUNET　1987InetClub　1992商用サービス)

情報セキュリティ研究開発企画・推進、事業支援(1995)

暗号・認証技術等の事業への活用推進　(1999IoT)

2007年　(株)IT企画設立

事業支援活動(顧問・相談役):2社(日、米)

大学教育活動(情報セキュリティ):九大、慶応

研究開発活動:中央大学研究開発機構、九州大学大学院

暗号・認証、秘密分散、バイオメトリクス、電子メールセキュリティ、

IoTシステムセキュリティ、FinTech(仮想通貨、ブロックチェーン)

ビッグデータ、AI　5分■

本日のご説明内容

［0］働き方改革とテレワーク

［1］テレワークに使用する
持出PCのセキュリティリスクおよび対策概要

［2］個人情報漏洩の現状・動向（統計データおよび事例）

［3］持出PCの紛失・盗難時の情報漏洩対策

［4］暗号技術と秘密分散技術
- 4.1 暗号技術の基本と応用例
- 4.2 秘密分散技術の基本と応用例
- 4.3 情報漏洩対策としての比較

［0］

働き方改革とテレワーク

「働き方改革」の狙い

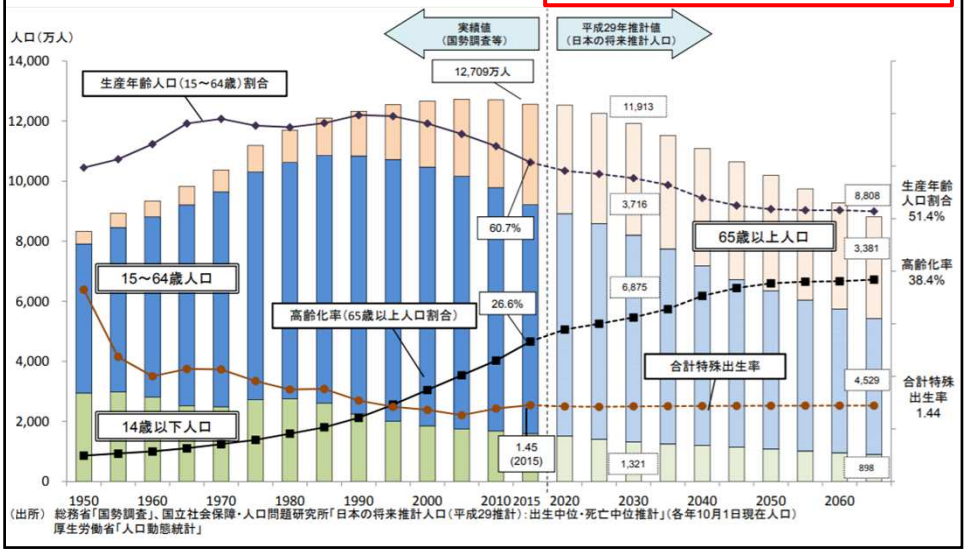
現状：
「少子高齢化に伴う生産年齢人口の減少」
「育児や介護との両立など、働く人のニーズの多様化」

課題：
「投資やイノベーションによる生産性向上」
「就業機会の拡大や意欲・能力を存分に発揮できる環境の構築」

「働き方改革」：以下の施策にて、この課題の解決を目指す
働く人の置かれた個々の事情に応じ、
多様な働き方を選択できる社会を実現し、
働く人一人ひとりがより良い将来の展望を持てるようにすること

日本の人口推移

生産年齢人口が2/3へ！
2015年：約7700万
2065年：約4500万

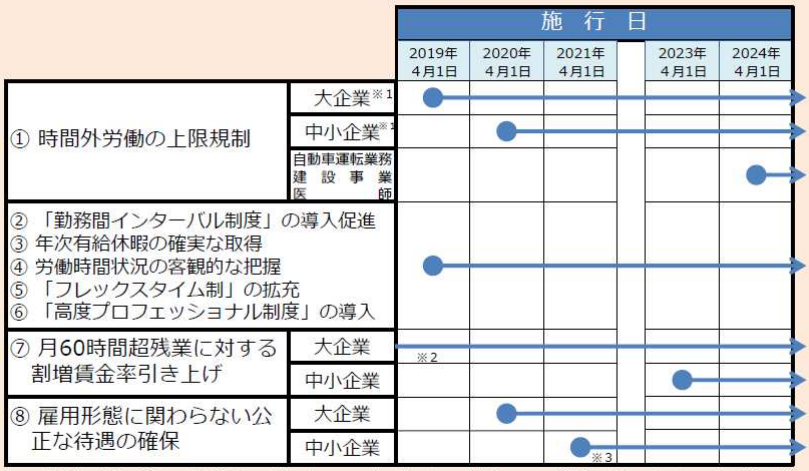


（出所） 総務省「国勢調査」、国立社会保障・人口問題研究所「日本の将来推計人口（平成29推計）：出生中位・死亡中位推計」（各年10月1日現在人口）
厚生労働省「人口動態統計」

「働き方改革を推進するための関係法律の整備に関する法律」

（2018年7月6日公布）

働き方改革関連法施行スケジュール



※1企業規模の定義は「中小企業基本法」の基準による。※2大企業はすでに実施済み。※3労働者派遣法の改正時期は大企業と同様。

働き方改革の三本柱

（1）労働時間の長時間化の是正

（2）正規・非正規の不合理格差の解消

（3）柔軟な働き方の実現

テレワーク

ICT（情報通信技術）を活用し、時間や場所を有効に活用

副業・兼業の促進

労働力の有効活用

シニア層の活用

労働人口の確保

テレワークワークとは

ICT（情報通信技術）を活用し、
時間や場所を有効に活用できる柔軟な働き方

企業にとってのメリット	従業員にとってのメリット
・人材の確保・育成	・ワーク・ライフ・バランスの向上
・業務プロセスの革新	・生産性の向上
・事業運営コストの削減	・自律・自己管理的な働き方
・非常時の事業継続性（BCP）の確保	・職場との連携強化
・企業内外の連携強化による事業競争力の向上	・仕事全体の満足度向上と労働意欲の向上
・人材の離職抑制・就労継続支援	
・企業ブランド・企業イメージの向上	

厚生労働省 「テレワークではじめる働き方改革」

都道府県別の一日当たりの通勤時間

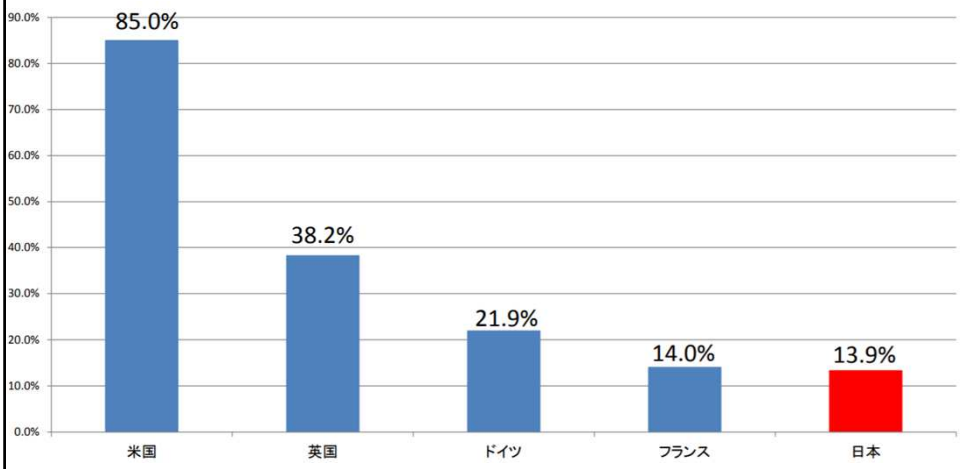
順位	都道府県名	通勤時間
1	神奈川県	1時間45分
2	千葉県	1時間42分
3	埼玉県	1時間36分
4	東京都	1時間34分
5	奈良県	1時間33分
6	大阪府	1時間25分
7	兵庫県	1時間21分
8	京都府	1時間20分
9	茨城県	1時間19分
9	愛知県	1時間19分

総務省統計局の社会生活基本調査

テレワークワークの三つの形態

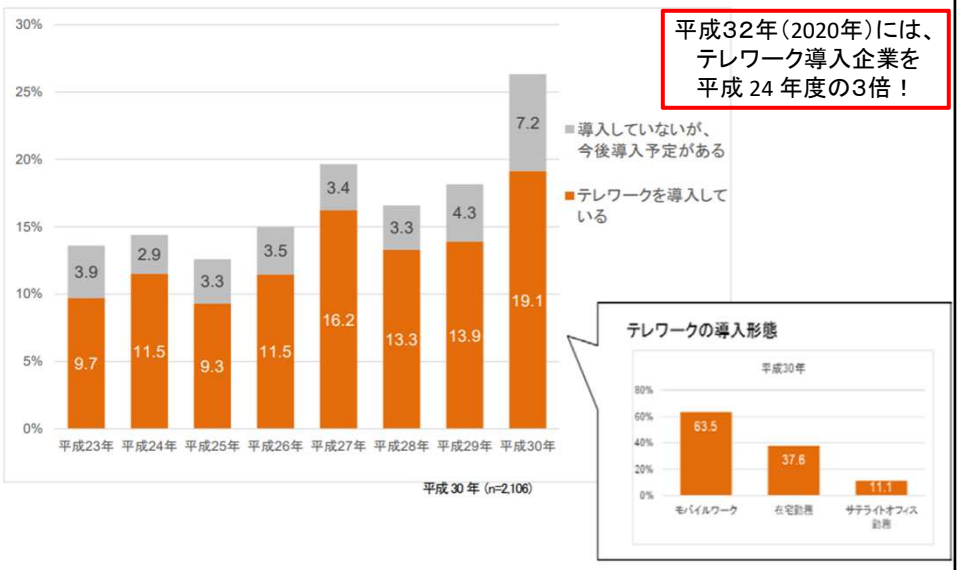
総務省「テレワークセキュリティガイドライン（第4版）」（平成30年）

テレワークの導入状況の国際比較
（2017年の企業導入率）



総務省「テレワークの最新動向と総務省の政策展開」

テレワーク導入状況（企業導入率）



平成32年（2020年）には、
テレワーク導入企業を
平成 24 年度の3倍！

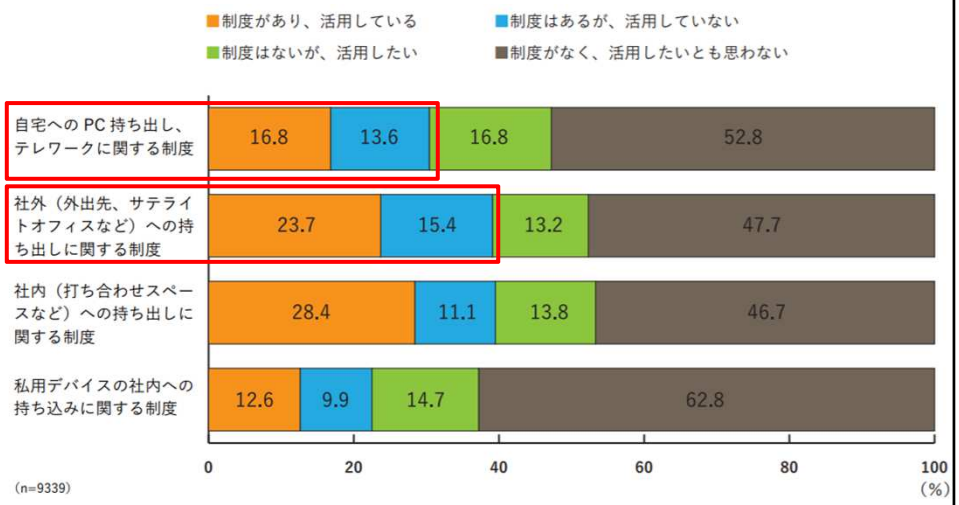
総務省「平成 30 年通信利用動向調査の結果（概要）」

10分■

［1］

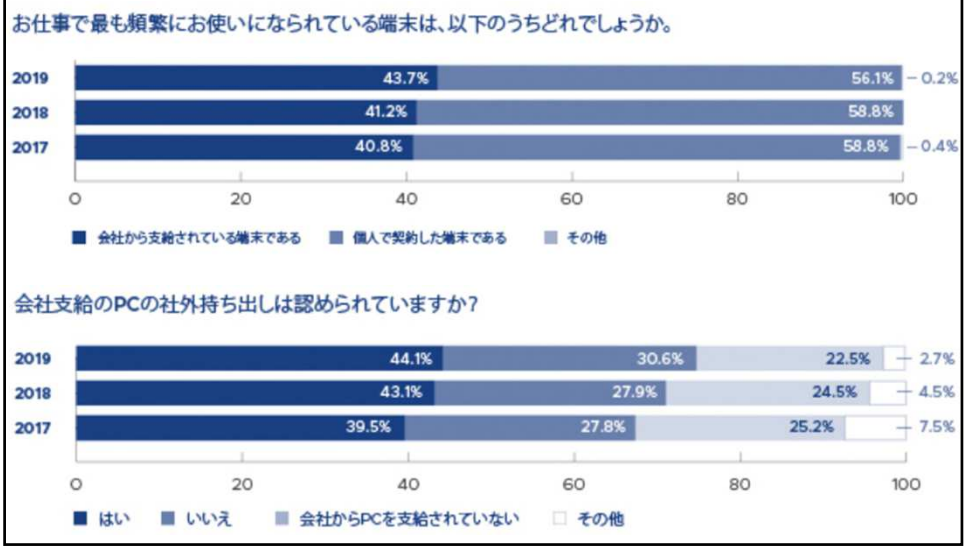
テレワークに使用する
持出PCの
セキュリティリスクおよび対策概要

PC持出制度、テレワーク制度の有無および PC持出活用状況、希望について

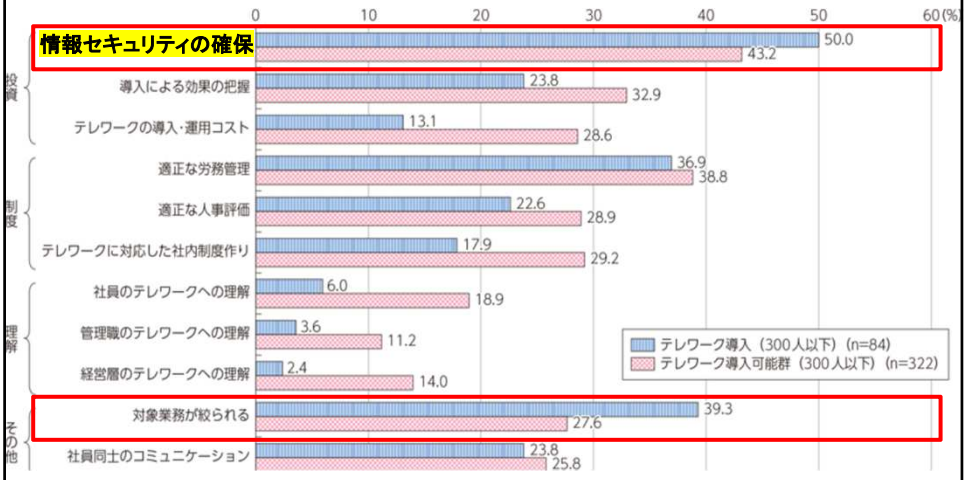


株式会社インサイトイメージ（調査：2016 年 12 月）

ビジネスにおけるモバイルの利用動向 （調査：2019年6月）

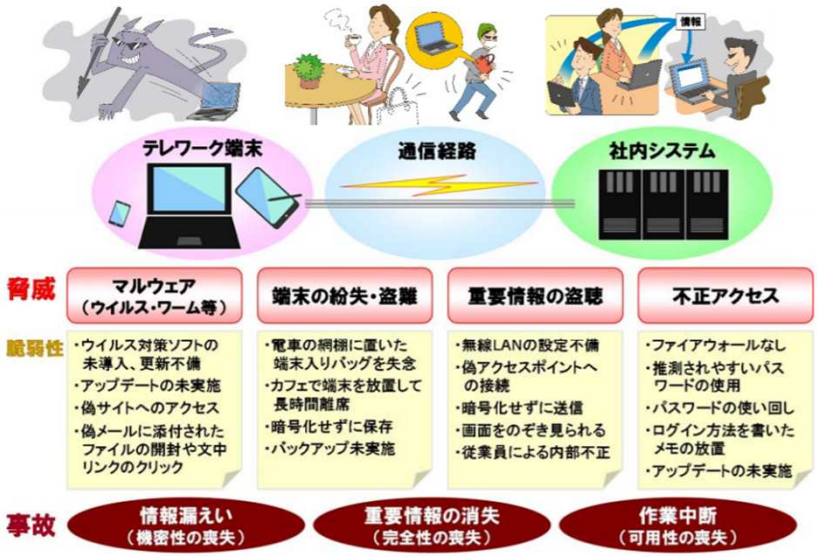


テレワークの導入にあたっての課題、導入するとした場合の課題



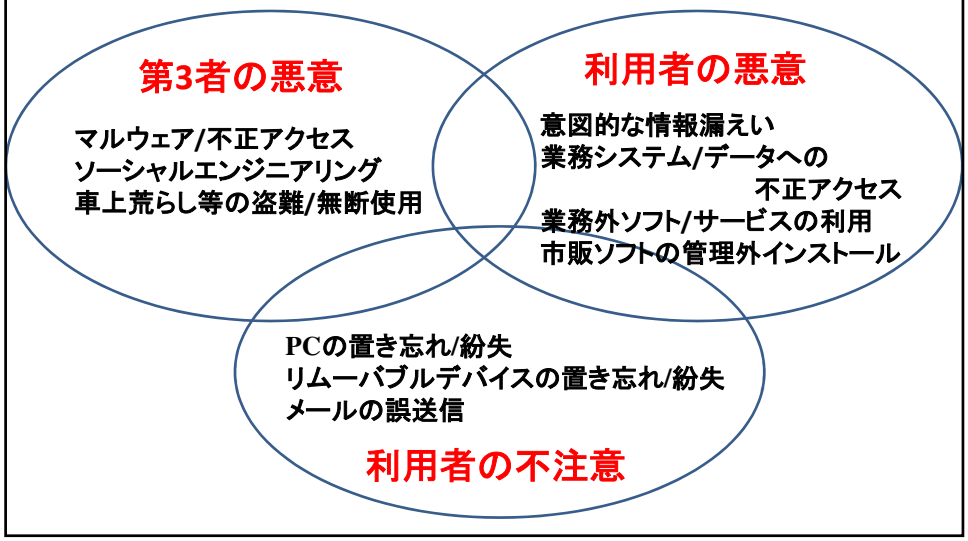
総務省「ICT利活用と社会的課題解決に関する調査研究」（平成29年）

テレワークにおけるセキュリティリスク概要

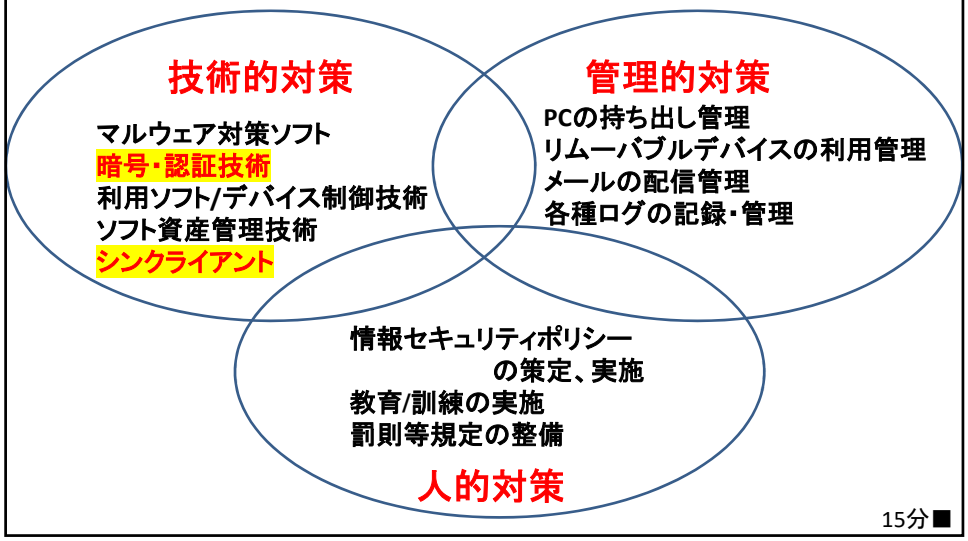


総務省「テレワークセキュリティガイドライン（第4版）」（平成30年）

持出PCのセキュリティリスク概要



持出PCのセキュリティ対策概要



15分■

［2］

個人情報漏洩の現状・動向（統計データおよび事例）

個人情報保護法

2003年（平成15年）成立

日本企業の多くは、過剰反応（PC持出の禁止まで）

2017年（平成29年）改正

主要な改正内容

①保有個人情報の件数による規制対象の限定の廃止（規制強化）

②個人識別符号の追加（規制強化）

③匿名加工情報の新設（規制緩和）

④要配慮個人情報の新設（規制強化）

個人データの漏えい等の事案が発生した場合等の対応

（平成 29 年個人情報保護委員会告示第1号）

①漏えい等事案が発覚した場合に講ずべき措置

②個人情報保護委員会等への報告

認定個人情報保護団体の対象事業者の場合は、その団体へ

個人情報漏洩インシデント概要

	2017年	2018年
漏洩人数	519万8142人	561万3797人
漏洩件数	386件	443件
想定損害賠償総額	1914億2742万円	2684億5743万円
一件当たりの漏洩人数	1万4894人	1万3334人
一件当たりの平均想定損害賠償額	5億4850万円	6億3767万円
一人当たりの平均想定損害賠償額	2万3601円	2万9768円

①個人情報漏洩インシデント件数は、約15%増
②1項目を除き、全て増加傾向

2018年 情報セキュリティインシデントに関する調査報告書（NPO日本ネットワークセキュリティ協会）のデータより作成
https://www.jnsa.org/result/incident/

紛失（事故）

2019-03-18 （岡崎市）
水道利用者の個人情報14.7万件含むタブレットを紛失
2019-03-02 （国立精神・神経医療研究センター）
患者の顔画像含むタブレット端末を紛失
2018-12-19 （東京ガス）
委託先作業員が顧客情報含む業務用端末を置き忘れ
2018-11-06 （朝日新聞）
個人情報含むPCを電車に置き忘れ（後に回収）
2018-11-02 （TBM）顧客情報619件含むノートパソコンを紛失
2018-08-27 （立命館宇治中高）オーストラリアでの海外研修で
引率教諭が生徒の個人情報が保存された
PC、USBメモリの入った鞄を置き忘れ
2018-07-11 （講談社）個人情報含むノートPCを都内で紛失

個人情報漏洩事件・事故関連記事の一覧（http://www.security-next.com/category/cat191/cat25）

盗難（事件）

2019-04-21 （大阪府）高校生徒の個人情報含むUSBメモリなどが盗難被害（車上荒らし）
2019-04-10 （福島県立医科大）複数医療機関の患者情報含むUSBメモリが海外（オランダ）の車内で盗難被害
2018-12-11 （長岡技術科学大）学生の個人情報含むPCが海外の学会会場で盗難被害
2018-10-11 （人事コンサルティング会社）顧客情報含むPCが盗難被害
2018-07-20 （上光証券）委託先で顧客住所録を含むパソコンが盗難被害（車上荒らし）
2018-07-09 （東大）個人情報含む教員の私物パソコンが学内で盗難
2018-06-01 （Peach航空）顧客の旅券情報含むPCが盗難被害
2018-05-16 （福岡大学筑紫病院）工事中に患者情報含むPCが盗難被害
2018-02-27 （久留米大）個人情報入りPCがドイツで盗難
2018-02-25 （名大病院）患者情報が勉強会帰りの寄り道で盗難被害

個人情報漏洩事件・事故関連記事の一覧（http://www.security-next.com/category/cat191/cat25）

業種別　漏洩件数

2017年	
業種内訳	（386件）
公務	110件
教育・学習支援業	60件
卸売業、小売業	33件
情報通信業	30件

2018年	
業種内訳	（443件）
公務	131件
教育・学習支援業	101件
情報通信業	33件
卸売業、小売業	31件

①教育・学習支援業が急増
②公務は恒常的に多い

2018年 情報セキュリティインシデントに関する調査報告書（NPO日本ネットワークセキュリティ協会）のデータより作成
https://www.jnsa.org/result/incident/

媒体・経路別　漏洩件数

2017年	
媒体・経路内訳	（386件）
紙媒体	150件
インターネット	87件
電子メール	77件
PC・可搬記録媒体	57件

2018年	
媒体・経路内訳	（443件）
紙媒体	132件
インターネット	118件
電子メール	95件
PC・可搬記録媒体	80件

①紙媒体による漏洩件数が最も多いが、減少傾向
②インターネット、電子メール、
PC・可搬記録媒体経由の漏洩は急増

2018年 情報セキュリティインシデントに関する調査報告書（NPO日本ネットワークセキュリティ協会）のデータより作成
https://www.jnsa.org/result/incident/

原因別　漏洩件数

2017年	
原因内訳	（386件）
誤操作	97件
紛失・置忘れ	84件
不正アクセス	67件
管理ミス	50件

2018年	
原因内訳	（443件）
紛失・置忘れ	116件
誤操作	109件
不正アクセス	90件
管理ミス	54件

①紛失・置忘れが最大の原因に！
紙媒体経由の漏洩が減少の中、
PC・可搬媒体の紛失・置忘れ急増か

2018年 情報セキュリティインシデントに関する調査報告書（NPO日本ネットワークセキュリティ協会）のデータより作成
https://www.jnsa.org/result/incident/

個人情報漏洩の現状から・・・

①個人情報以外の企業秘密情報等の漏洩は、
報告義務が無いため正確なデータは存在しないが、
個人情報漏洩事故・事件以上に発生していると推測

②テレワークにより、持出PCの活用が増加し、
持出PCの「紛失・置忘れ」、「盗難」による
情報漏洩事故・事件も増加するものと推測

20分■

［3］

持出PCの
紛失・盗難時の情報漏洩対策

持出PCの紛失・盗難時の情報漏洩対策一覧

（1）パソコンの紛失を防ぐ仕組み

＊紛失・忘れ物防止タグ/シール

（2）パソコンが紛失・盗難されても、
そのパソコン内へのアクセスを防ぐ仕組み

＊ログイン認証（記憶、持物、生体特徴）

＊リモートロック

（3）紛失・盗難パソコン内へアクセスされても、
情報の漏洩を防ぐ仕組み

＊**データの暗号化、秘密分散**

＊リモートワイプ

（4）紛失・盗難パソコン内へアクセスされても、
情報の漏洩が発生しえない仕組み

＊**シンクライアント**

シンクライアントの分類

（1）ネットブート型

サーバ上にあるOSやアプリケーションをクライアント上で実行

（2）画面転送型

サーバベース：アプリケーションをサーバ上で実行
一つのサーバを複数人で共同利用する方式

ブレードPC：クライアントごとに専用ブレードPCを用意
アプリケーションをブレードPC上で実行

VDI（Virtual Desktop Infrastructure）：
サーバ上に仮想のデスクトップ環境を構築
アプリケーションを仮想マシン上で実行

シンクライアントの特徴

	ネットブート型	画面転送型		
		サーバベース	ブレードPC	VDI
導入実績	△	◎	○	◎
集約率	△	◎	△	○
アプリケーションの互換性	◎	△	◎	○
既存PCの利用	○	◎	△	◎
個別アプリのインストール	○	×	○	○

https://sandi.jp/column/corpus-thinclient/20140909.html を参考に作成

シンクライアントの普及・活用状況・動向

（IDC Japanの報告より）

（1）2016年6月：法人向けクライアント市場の仮想化導入率
2020年には42.3%へ拡大すると予測（2014年：25.7%）

（2）2018年7月：2017年 国内クライアント仮想化ソフトウェア市場
267万5,885ライセンス、前年比12.0%増 （28万6702ライセンス）
（サーバベース仮想化、デスクトップ仮想化（VDI）の順）

（3）2019年6月：2023年のクライアント仮想化利用ユーザ数
772万人まで拡大と予想
（2018年の実績では、「金融」「官庁／自治体／教育」「製造」）

（4）シンクライアント専用端末は、2018年の出荷台数
総計24万3512台で、前年比19.3%増 （3万9395台）

クライアントのタイプ別分類

シンクライアント：データ管理、処理機能をサーバ側に集中させ、
必要最小限の機能を提供するクライアントコンピュータ
ファットクライアント：サーバとは独立に
データ管理、処理機能を提供するクライアントコンピュータ
データレスクライアント：データ管理はサーバ側に集中させ、
処理機能を提供するクライアントコンピュータ

比較項目	ファット クライアント	シン クライアント	データレス クライアント
セキュリティリスク	大	小	小
コスト	小	大	中
生産性	高	低	低
快適操作性	高	低	低

ファットクライアントの紛失・盗難時の情報漏洩対策

（1）なぜ、ファットクライアントなのか
①働き方改革➔テレワークの比率増大
生産性の維持➔シンクラからファットへ
②セキュリティ技術・システムの充実
➔持出ファットクライアントのリスクへの対応が容易に
➔ファットクライアント活用の動きも

（2）ファットクライアント向け紛失・盗難時の情報漏洩対策
①暗号技術の利用
ハードディスク/ファイルの暗号化鍵、復号鍵の別管理
②秘密分散技術の利用
ハードディスク/ファイルの秘密分散、分散片の一部を別管理

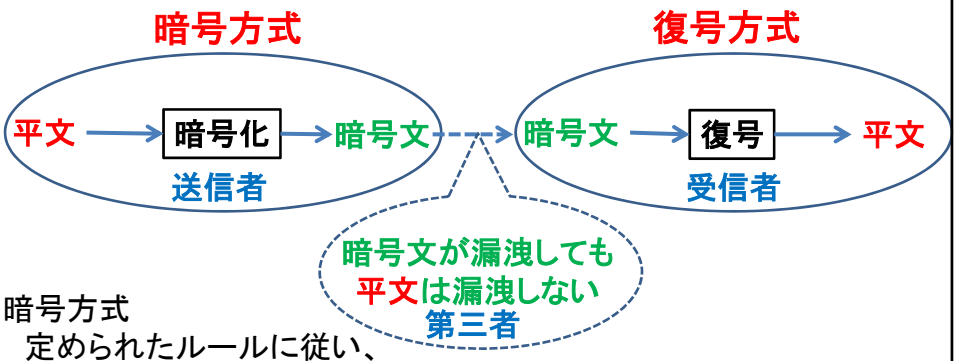
25分■

[4]

暗号技術と秘密分散技術

4.1 暗号技術の基本と活用事例
4.2 秘密分散技術の基本と活用事例
4.3 情報漏洩対策への適用

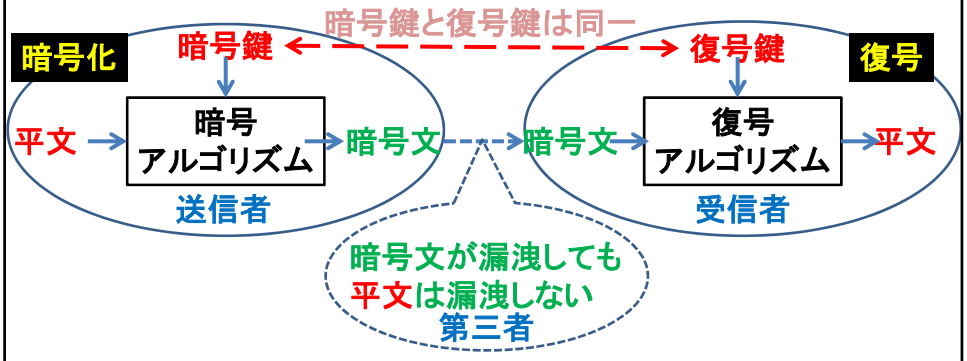
暗号技術とは



暗号方式
　定められたルールに従い、
　内容が分かる文章（平文）を、内容の分からない文章（暗号文）へ
　変換する方式
復号方式
　暗号文を元の平文へ戻す方式（それぞれの暗号方式に対応）
暗号技術
　平文を暗号化でき、また復号できる、暗号方式および復号方式の対

共通鍵暗号方式

暗号鍵と復号鍵が同一



共通鍵暗号方式の課題

あらかじめ、通信相手と暗号鍵（復号鍵）を共有しておく必要がある

共通鍵暗号方式

代表的な暗号方式と活用事例

米国

DES：鍵長56ビット、1976年米国連邦標準、2005年標準から除外

AES：鍵長128、192、256ビット、2001年米国連邦標準

日本

NTT：1985年FEAL（64ビット）　＜CRYPTREC＞

三菱：1995年MISTY（128ビット）2003年Camellia（128ビット）

東芝：1999年Triplo（128ビット）、2003年Hierocrypt-3（128ビット）

日本での活用事例

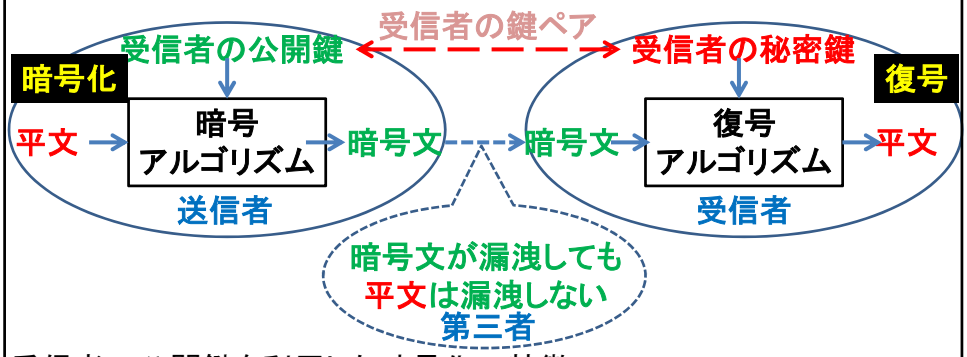
有料放送（デジタル：2000年）：
限定受信システム（CAS：Conditional Access System）

ノンストップ高速道路料金収受（1997年）：ETC（Electronic Toll Collection）

PCでDVD視聴（1998年）：DTCP（Digital Transmission Content Protection）

公開鍵暗号方式

暗号鍵と復号鍵が異なる



受信者の公開鍵を利用した暗号化の特徴

公開されている公開鍵により暗号化された暗号文は、
対応する秘密鍵を所有する受信者しか復号できない

受信者の公開鍵を利用した暗号化の課題

公開されている受信者の公開鍵が正しいことを確認する必要がある

公開鍵暗号方式

代表的な暗号方式と活用事例

主要な公開鍵暗号方式

1978年RSA暗号：大きな素数の積の
素因数分解問題の難しさを利用

1985年楕円曲線暗号：楕円曲線上の
離散対数問題の難しさを利用

日本での活用事例

2001年クレジットカード（EMV仕様、RSA暗号）

2006年ICパスポート（ICAO準拠、RSA暗号、楕円曲線暗号）

2016年マイナンバーカード（RSA暗号）

暗号技術まとめ

(1)暗号技術

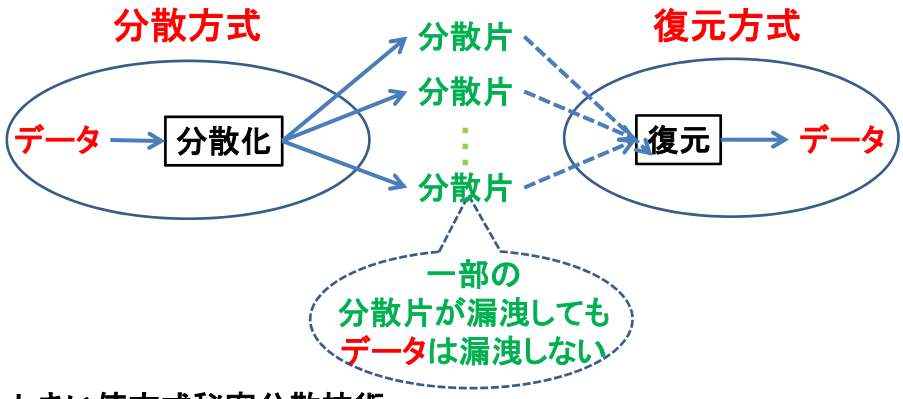
共通鍵暗号:DES(1976)、AES(2001)
NESSIE暗号群(2003)、CRYPTREC暗号群(2003)
公開鍵暗号:DH鍵共有(1976)、RSA(1978)、楕円曲線(1985)

(2)最近の動向(研究開発、応用)

IoT向け軽量暗号:CRYPTRECにて評価、
暗号技術ガイドライン(軽量暗号)に結果記載
耐量子計算機暗号(PQC):NISTにて標準化中
{LOTUS(NICT)、Giophantus(東芝、他)等、日本からも応募}
暗号化状態処理:基礎研究・実用化研究が中心だが商品化も。
{NTT、NEC、産総研が秘密計算(統計分析)を実用化}

35分■

秘密分散技術とは



しきい値方式秘密分散技術
分散片の総数(n)の内、あらかじめ定められた数(k)の分散片から、元のデータを復元できる方式(k未満の分散片では復元できない)

AONT方式秘密分散技術
全ての分散片がそろってはじめて、元のデータを復元できる方式

しきい値方式秘密分散技術
一定数の分散片による復元

Shamirのしきい値秘密分散法 (k,n)

$f(x)=S+a_1x+a_2x^2+\cdots+a_{k-1}x^{k-1}$

S：秘密の情報

$a_1,\cdots,a_{k-1}$：乱数で生成

n個の分散片$w_1,\cdots,w_n$の生成

$w_i=f(i)$ $i=1,\cdots,n$

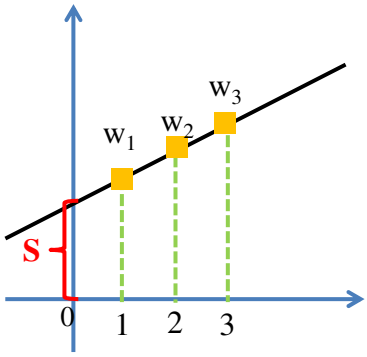
k個の分散片w_j, $j=\{i_1,\cdots,i_k\}$からの復元

（ラグランジュ補間式を利用）

$S=f(0)$

$=\Sigma_{i\in j}w_i\Pi_{i'\in j\neq i}(-i'/(i-i'))$

(2,3)の例 $f(x)=S+a_1x$



しきい値方式秘密分散技術
方式発表の歴史および応用分野

1979年：Shamirが、多項式を利用した**しきい値秘密分散法**を発表(k,n)

（同時期にBlakleyが、異なる方式によるしきい値秘密分散法を発表）

1984年：Yamamotoが、**ランプ型しきい値秘密分散法**を発表（k,L,n)

（同時期にBlakley-Meadowsも同様の方法を発表）

ランプ型しきい値秘密分散法のメリット

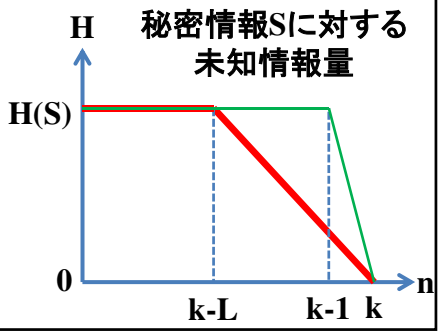
$H(W_i)=H(S)/L$

応用分野

情報報保護、データ消失リスク低減を目的とした

＊分散ストレージサービス

＊バックアップサービス



AONT方式秘密分散技術

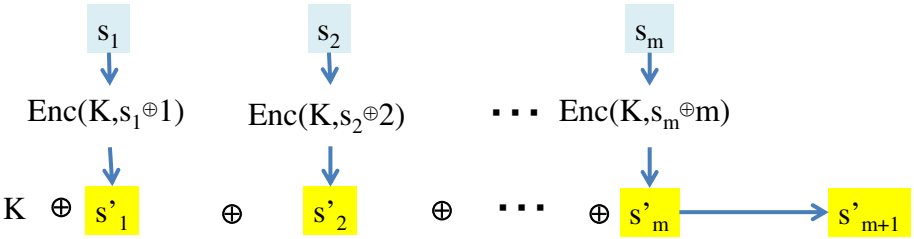
全数の分散片による復元

RivestのAONT（all or nothing transform）秘密分散法

秘密情報Sの n ビット単位の m 個の分割片を s_i（i=1,・・・,m）

乱数で生成する暗号鍵をK（Kの鍵長はn ビット）

分散片の生成



分散片からの復元

$K=s'_1+s'_2+\cdots+s'_m+s'_{m+1}$

$s_i=Dec(K, s'_i)\oplus i$

AONT方式秘密分散技術

方式発表の歴史および応用分野

1997年：RivestがAONT方式を考案

2000年：DesaiがCTRT-AONT方式を提案、安全性を証明

2018年：ZenmuTech社がZENMU-AONTを提案、
安全性を証明の上、実装
（CTRT-AONTの改良版、鍵長を128ビットから256ビットへ）

応用分野

情報保護を目的とした

クライアントPCの情報保護

メール等の通信情報の保護

IoT収集データの保護

秘密分散技術まとめ

（1）秘密分散技術

しきい値方式：Blakley/Shamir考案（1979）、
ランプ型しきい値分散法（1985、山本）

AONT方式：Rivest考案（1997）、CTRT-AONT（2000、Desai）

（2）最近の動向（研究開発、応用）

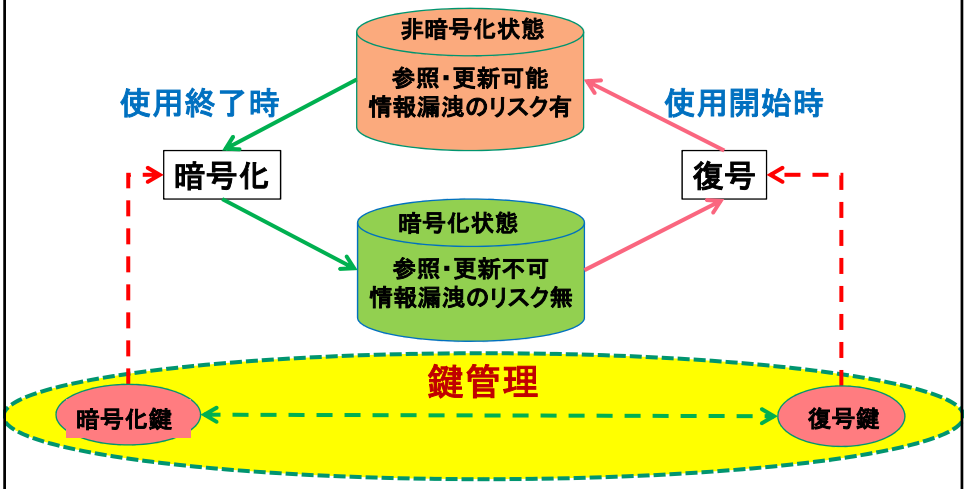
しきい値方式：ISOが秘密分散技術の標準規格
ISO/IEC 19592-2:2017を発行
{5つの秘密分散方式が採択され、NTT独自方式も採択}

AONT方式：実用的パッケージ製品が市場へ
{ZENMU-AONT（CTRT-AONTの改良版）}

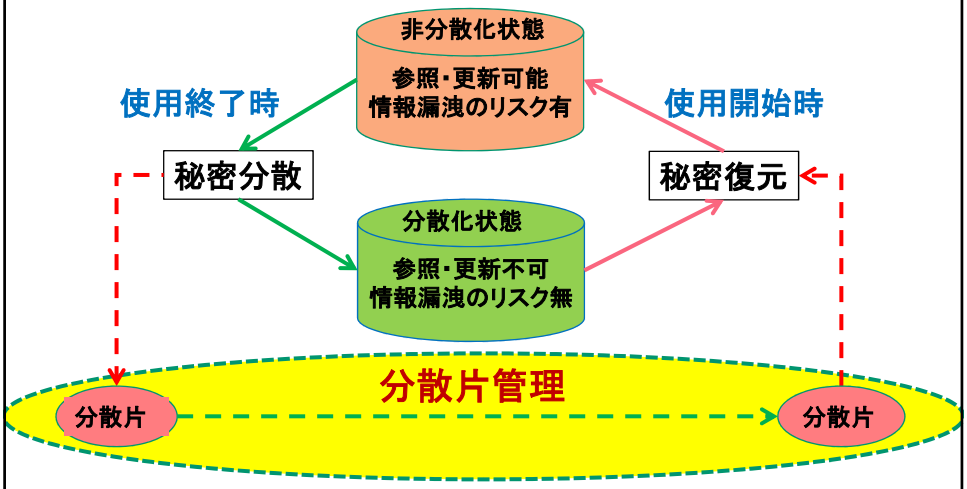
秘密分散状態処理：基礎研究・実用化研究が中心だが商品化も。
{秘密計算システム 算師®（NTT）等}

45分■

暗号化による
紛失・盗難PCからの情報漏洩対策



AONT方式秘密分散による紛失・盗難PCからの情報漏洩対策



情報漏洩対策としての比較

（1）機能はほぼ同等

PC外管理情報（復号鍵、分散片）をしっかり管理していれば、
持出PCの紛失・盗難による情報漏洩は防げる

個人情報保護委員会等への報告を要しない場合に該当、と推定

（注1）暗号化の場合、①適切な暗号アルゴリズムの適切な実装、
②鍵の安全な管理

（注2）AONT方式秘密分散の場合、①適切な暗号アルゴリズムの
適切な実装、②鍵を秘匿する分散片（s'_{m+1}）の安全な管理

（2）運用管理負担は実装に依存

PC外管理情報の安全な管理のための利用者、運用組織の負担

（3）利用時の負担は実装に依存

操作性能の良さ（生産性、快適性）

待ち時間の少なさ（利用開始時、利用終了時）

おわりに

[0]働き方改革とテレワーク
[1]テレワークに使用する持出PCのセキュリティリスクおよび対策概要
　　リスク：第3者の悪意、利用者の不注意、利用者の悪意
　　対策：技術的対策、管理的対策、人的対策
[2]個人情報漏洩の現状・動向（統計データおよび事例）
　　持出PC特有の事故・事件：紛失・盗難多発・増加の傾向、事例
[3]持出PCの紛失・盗難時の情報漏洩対策
　　シンクライアントの分類・動向
　　ファットクライアントのセキュリティ対策
[4]暗号技術と秘密分散技術
　4.1　暗号技術の基本と活用事例
　　共通鍵暗号方式、公開鍵暗号方式
　4.2　秘密分散技術の基本と活用事例
　　しきい値方式、AONT（all or nothing transform）方式
　4.3　情報漏洩対策としての比較
　　機能：ほぼ同等　運用・利用者負担、利便性は実装依存

終

ご清聴、ありがとうございました