安全マネジメント　第4回

深層防護
Defense-in-Depth

長岡技術科学大学
大学院技術経営研究科
システム安全専攻
実務家教授　山形　浩史
yamagata@vos.nagaokaut.ac.jp

深層防護（Defense-in-Depth）

- もともとは、ヨーロッパにおける軍事戦略の一つ
- 一般産業などにおいても、多重防護、冗長システムとして広く用いられている

江戸城の深層防護

深層防護の層構造

基本：二層構造

通常運転

①事故の発生防止

事故

②事故の影響緩和

標準：三層構造

通常運転

①通常状態からの逸脱防止

異常・故障

②事故への拡大防止

事故

③事故の影響緩和

大プラント：五層構造

通常運転

①通常状態からの逸脱防止

異常・故障

②事故への拡大防止

事故（物損）

③事故の影響緩和

事故（人身）

④工場外への影響緩和（離隔）

工場内

工場外へ被害

⑤避難・防災

基本：二層構造

通常運転

①事故の発生防止

①目を離さない

急にトイレに！

小野市消防本部HP

事故

②事故の影響緩和

②消　　火

鳥取県東部広域行政管理組合HP

標準：三層構造

通常運転

①通常状態からの逸脱防止

異常・故障

②事故への拡大防止

事故

③事故の影響緩和

①自動温度調節機能

故障！

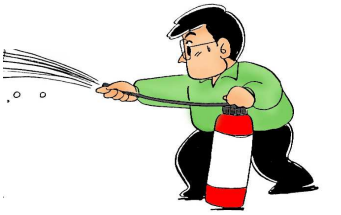
温度上昇

②目を離さない

急にトイレに！

小野市消防本部HP

③消　　火



鳥取県東部広域行政管理組合HP

大プラント：五層構造

工場内

通常運転

①通常状態からの逸脱防止

①自動温度調節機能

温度上昇 → 故障！

異常・故障

②事故への拡大防止

②温度検知器・操業停止

故障！

事故（物損）

③事故の影響緩和

③火災検知、消火

従業員負傷

延焼！

事故（人身）

④工場外への影響緩和（離隔）

④防火帯、コンビナート立地

風向！

工場外へ被害

住宅地に煙・異臭・有害物質

⑤避難・防災

⑤自治体による避難誘導

設計基準事象と事故発生防止策

「不測の事態に備えよ、想定外に対処せよ」と言われても設計はできない

設計基準事象：過去の経験や合理的な想定から、設計として考慮すべき事象

事故発生防止策：設計基準事象が発生しても、通常状態に戻る又は軽微な補修で通常状態に戻るよう事前に対策を取る

例：　漏電・短絡は、過去にも発生しているので設計に考慮する
事故（火災）の発生防止策として、ブレーカーを設置する

震度7の地震は、土地を買った県では発生していないが、日本では何度か起こっているので、設計に考慮する
事故（倒壊）の発生防止策として、震度7に耐えれるよう新居を設計する

設計基準事故と事故影響緩和策

事故発生防止策を取っていても、事故は発生することがある

設計基準事故：過去の経験や合理的な想定から、設計として考慮すべき事故

事故影響緩和策：設計基準事故が発生しても、甚大な被害とならないよう事前に対策を取る

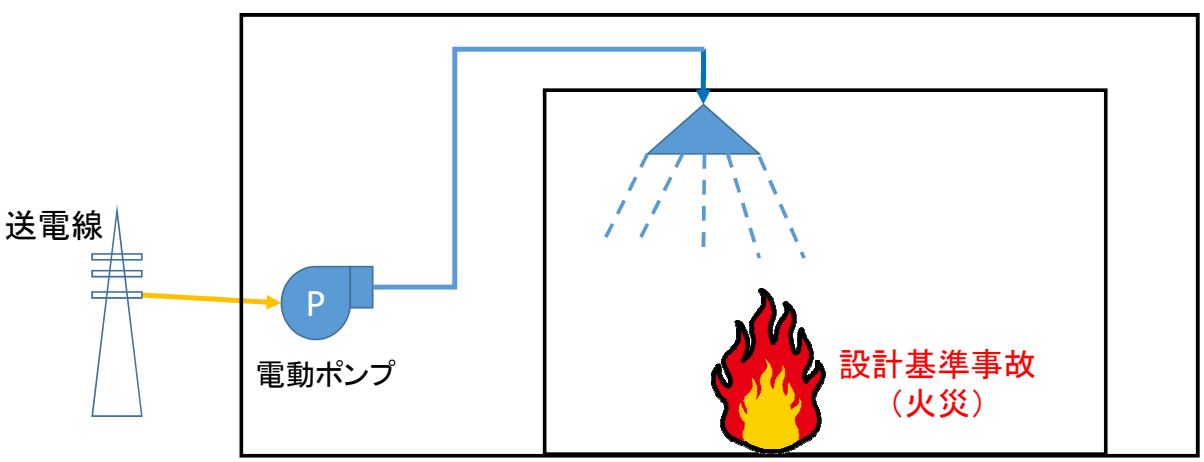
例：　事故（火災）は、過去にも発生しているので設計に考慮する
火災の拡大防止策として、スプリンクラーを設置する（壁は焦げるが全焼しない）

地震による事故（倒壊）は、土地を買った県では発生していないが、日本では何度か起こっているので、設計に考慮する
事故（倒壊）の拡大防止策として、寝室とリビングは強固な鉄骨フレームにする
（瓦が落ち窓は割れるが、在宅中多くの時間を過ごす場所では、怪我をしない）

設計基準事故と事故影響緩和策

例：　事故（火災）は、過去にも発生しているので設計に考慮する
火災の拡大防止策として、スプリンクラーを設置する（壁は焦げるが全焼しない）

Discussion：信頼できますか？



各層の信頼性向上

① 多重性： 同じものが複数
（ランダム故障対策）

②多様性： 構造や動作原理が異なる
（共通要因故障対策）

③独立性： お互いに物理的に分離
（共通要因故障対策）

④位置的分散： お互いに離れる
（想定外への強靭性）

例：消防ポンプ

電動ポンプが1台 — たまたま故障

電動ポンプが2台 — 停電で2台とも使えない

電動ポンプが1台
ディーゼルポンプが1台 — 火事で2台とも使えない

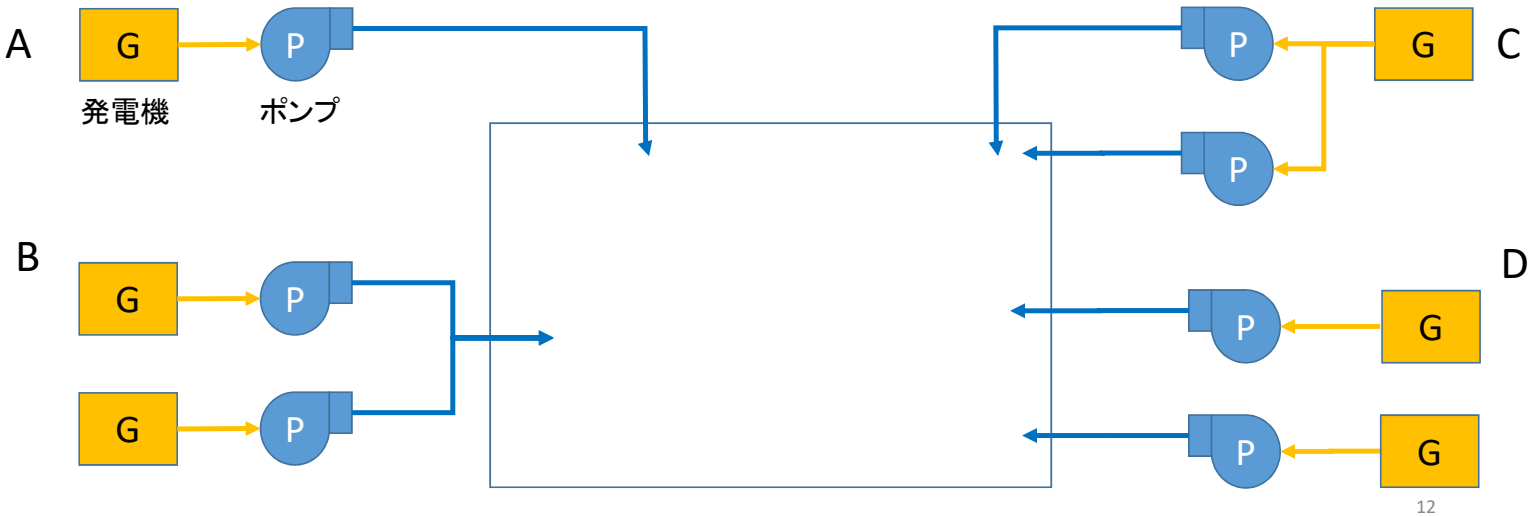
電動ポンプが1台
ディーゼルポンプが1台
の間に防火壁 — 想定外の爆発で使えない

電動ポンプが1台
ディーゼルポンプが1台
互いに離れた別室に

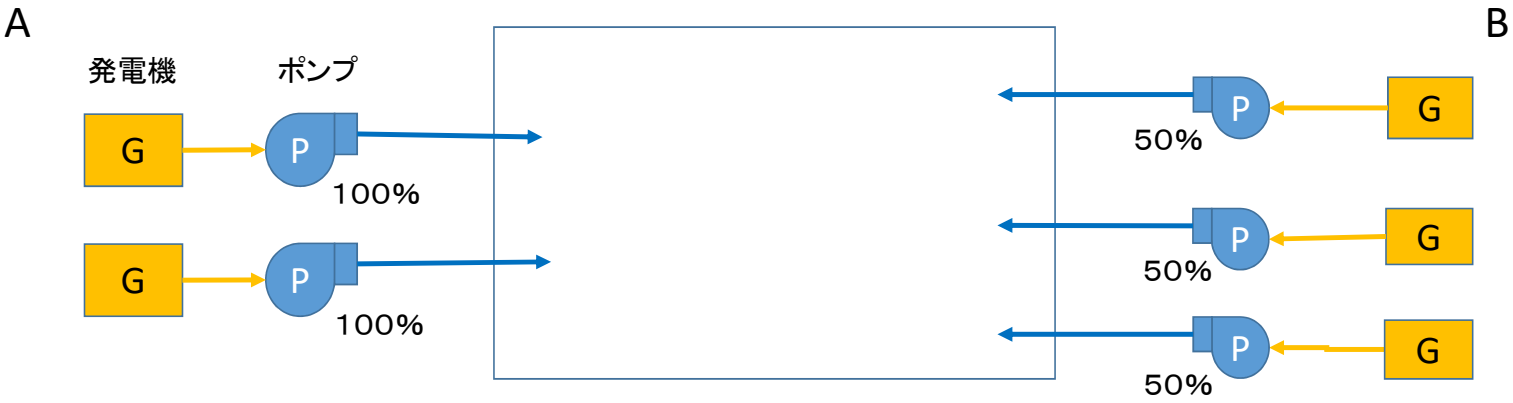
各層の信頼性向上（多重性）

単一故障基準： もっとも重要な箇所（任意の一か所）を損傷させてもシステムが機能する

Discussion: どれが単一故障基準を満たしている？

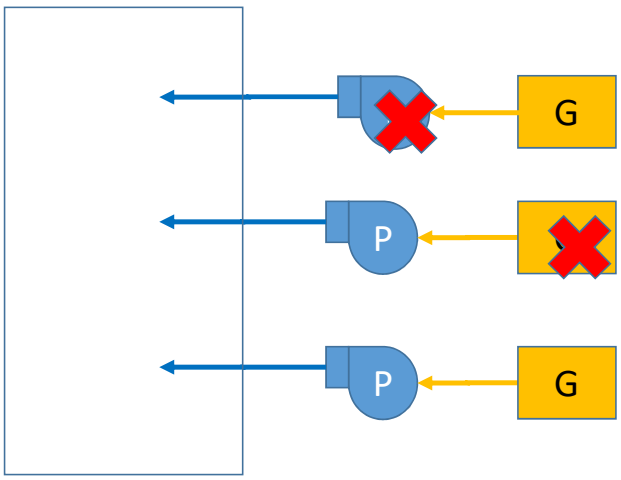


Discussion:
単一故障基準を満たしているか？
信頼度が高い（失敗確率が低い）のはどっち？



各層の信頼性向上（多重性）

二重故障基準：任意の2箇所を損傷させてもシステムが機能する



注意：
消火という目的が同じなので、層は同じ。
左は、多重であっても多層ではない。

層が異なる例：
① 火災の発生防止（不燃材、漏電防止）
② 火災の影響緩和（検知、消火）
③ 避難
④ 救出

各層の信頼性向上（多様性）

動的機器 と *静的機器*

ポンプ

給水塔

配管

電動弁
(大和バルブHP)

安全弁
(岡野バルブHP)

ラプチャー
ディスク
(日立造船HP)

高信頼度

静的機器の信頼性

一般的に静的機器の信頼性は高い

ただし、過信は禁物

点検を怠ってはいけない

日本原燃株式会社
濃縮工場排気ダクト
(日本原燃HP)

動力源の信頼性（多様性）

電動ポンプと発電機　　ディーゼル駆動ポンプ　　人力ポンプ　　重力注入

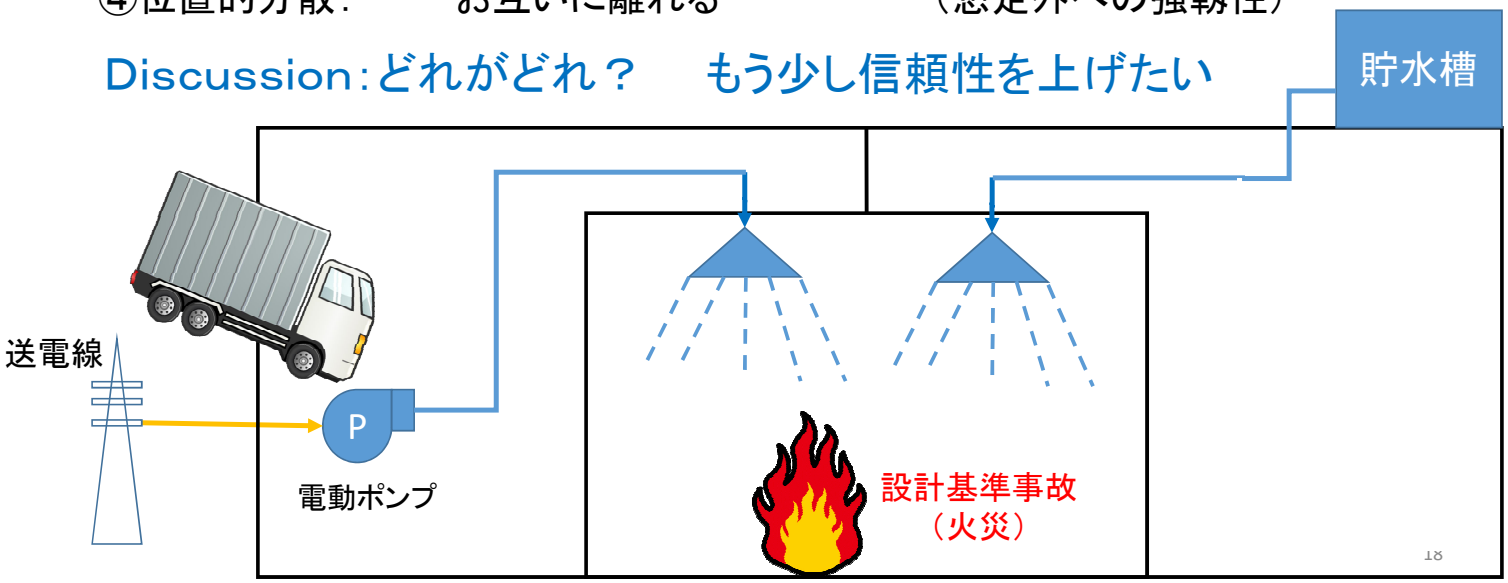
出典：消防博物館HP

出典：鴻池組HP

各層の信頼性向上（まとめ）

①多重性：	同じものが複数	（ランダム故障対策）
②多様性：	構造や動作原理が異なる	（共通要因故障対策）
③独立性：	お互いに物理的に分離	（共通要因故障対策）
④位置的分散：	お互いに離れる	（想定外への強靭性）

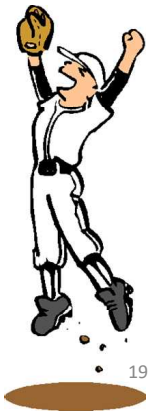
Discussion：どれがどれ？　もう少し信頼性を上げたい



層間の独立性

前段否定：前の層が万全であっても、失敗するとして対策を取る
後段否定：後の層が万全であっても、頼らない

各層で最善を尽くす



層間の独立性

Discussion: どちらがシステムといて強靭か？

日本の列車

運行管理技術は高い評価

事故発生防止技術は高い信頼性

ATSなど

事故が起こると車体は弱い

日比谷線事故

欧米の列車

事故が起きても車体は頑丈

衝突実験

層間の独立性

- 事故の発生防止に重きを置きすぎていないか。
  - 想定外に、事故の発生防止対策は機能しない。
  - リスク評価を行えるのは、想定できる事象のみ
- 事故の発生防止に重きを置いてもいいが、事故の影響緩和を忘れてはいけない。

設計基準超

設計基準： 安全なものを造るために設計において考慮する基準

例： 地震動、風速、雨量、雷、火災など

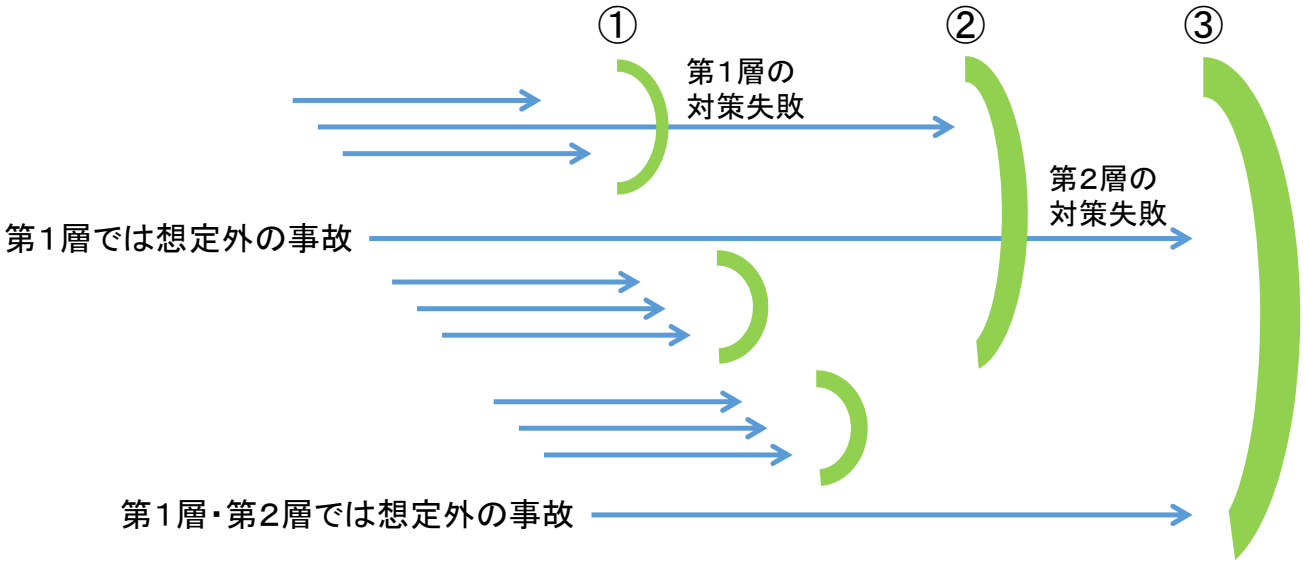
設計基準超： 設計基準を超える外力が加わることは否定できない
多くの場合にコストとの兼ね合いで設計基準を過大にすることはできない

Discussion： 設計基準の設定レベルは？超えたときの対策は？

1. 保険： 震度7に耐える家を買い、それ以上の地震で家が倒壊すれば地震保険でカバー
2. 減災： 高い防潮堤を造るより、避難路の整備や高台移転
3. 緩和： 事故により機械は壊れても、人命を脅かさない防護策

後段の層ほど幅広く

想定外は起こりえるので、後段の対策ほど幅広い事象に対応できるようにする

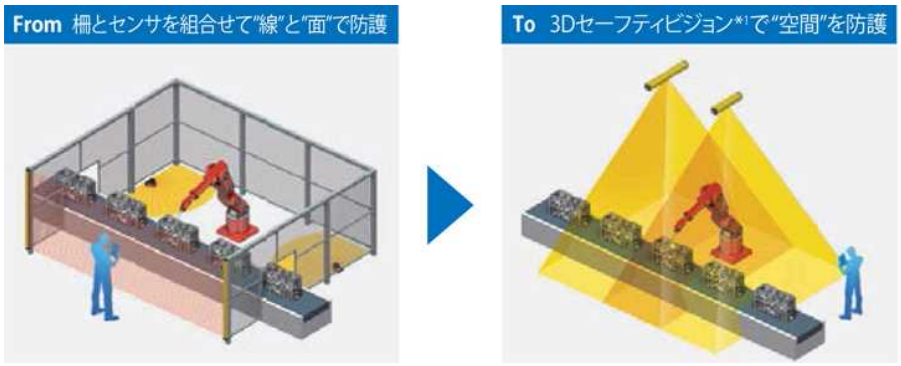


後段の層ほど幅広く
（例：禁煙の倉庫での火災対策）

火災の原因		火災発生防止対策
漏電	←	配線交換
雷サージ	←	避雷針
モーター加熱	←	整備、温度計
揮発油	←	持ち込み禁止
たばこのポイ捨て（想定外）		

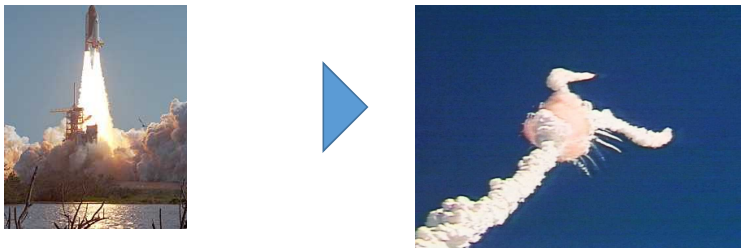
火災影響緩和対策
（原因によらず消火）

Discussion：それでも離隔は必要か？

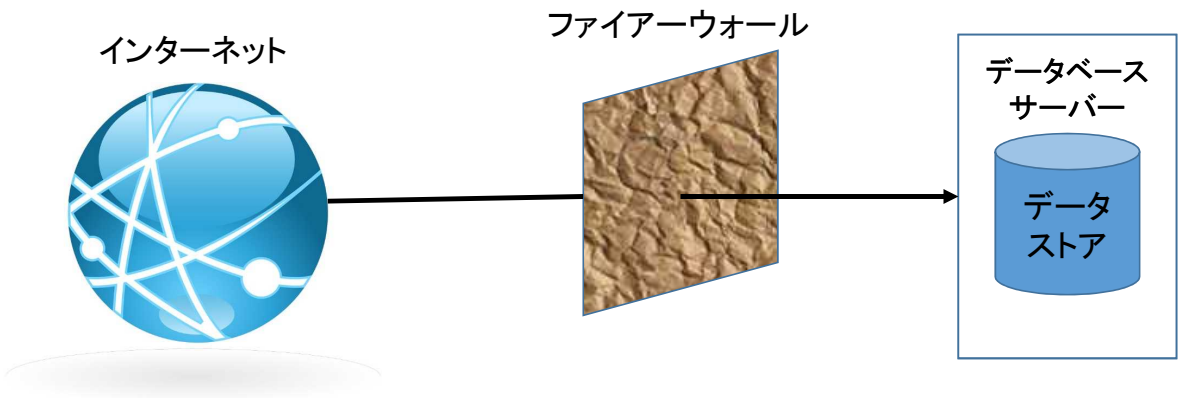


出典：OMROM HP

Discussion：それでも脱出装置は必要か？

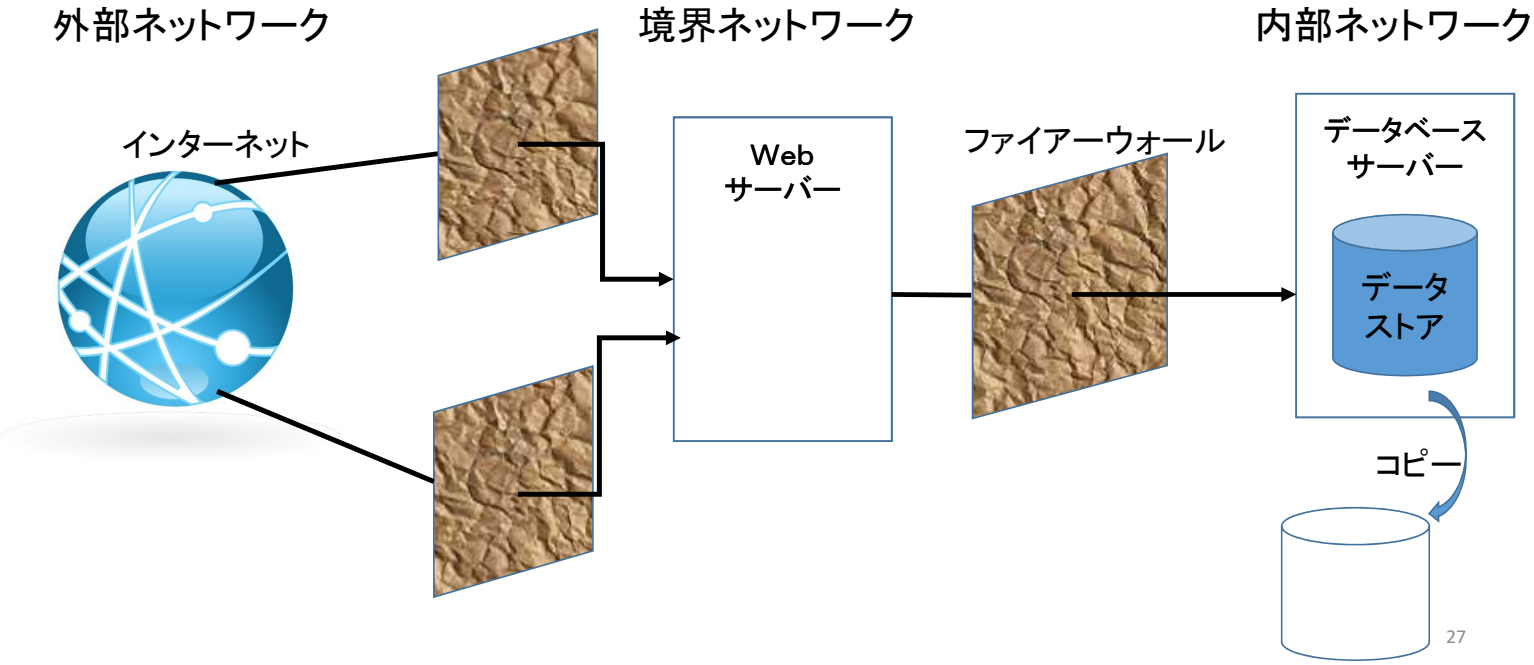


Discussion： データを守る方法？



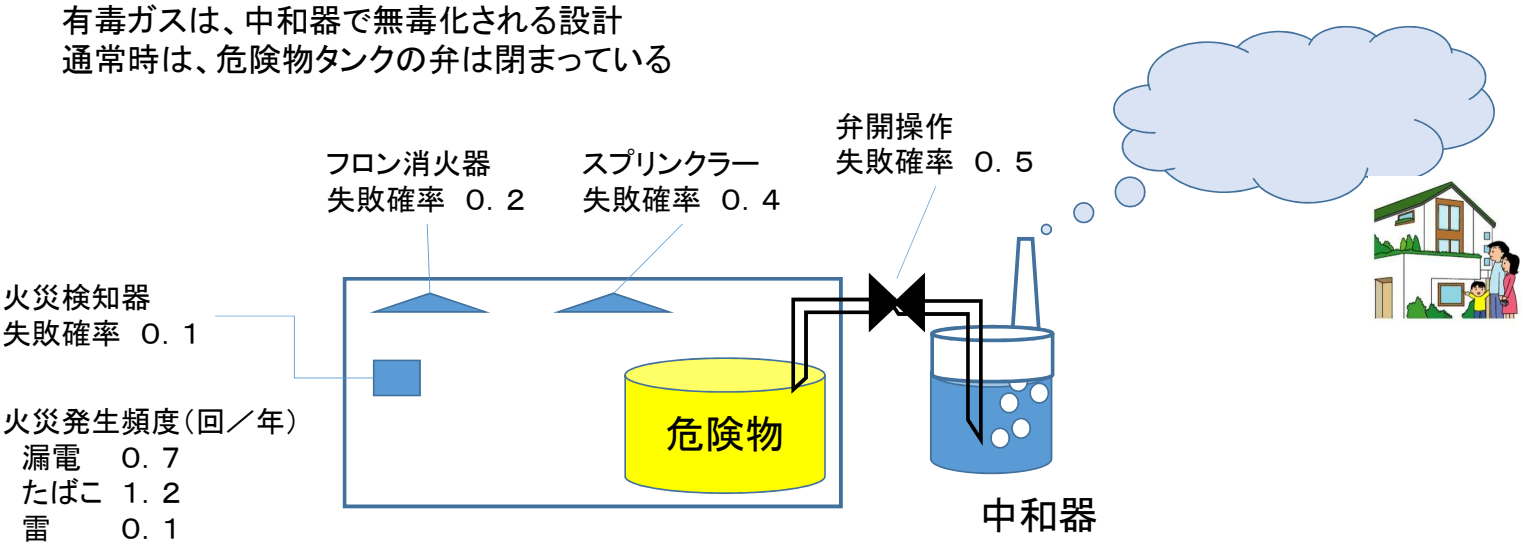
データをいつでも使えること（可用性）にも考慮してください

Discussion： データを守る（例）

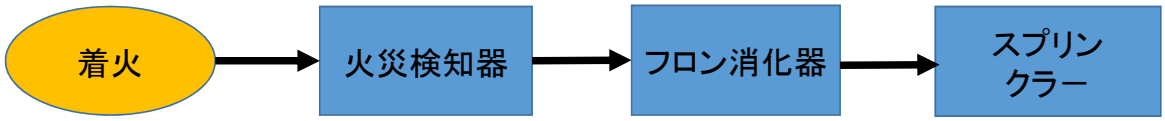


Discussion: 有毒ガスから住民を守るには イベントツリーを作成し、分析

工場内の危険物は加熱されると有毒ガスを発生
有毒ガスは、中和器で無毒化される設計
通常時は、危険物タンクの弁は閉まっている

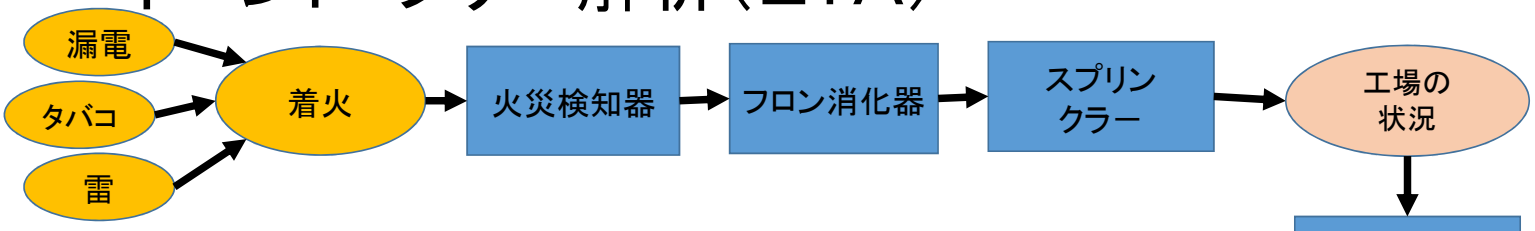


（参考） イベント・ツリー解析（ETA）



起因事象	火災検知器	フロン消化器	ｽﾌﾟﾘﾝｸﾗｰ	
		成功		消火
		0.8		1.44
	成功		成功	消火・水浸し
	0.9		0.6	0.216
		失敗		
火災発生		0.2		
2 回/年			失敗	全焼
			0.4	0.144
	失敗			全焼
	0.1			0.2
		合計全焼頻度		0.344 回/年

イベント・ツリー解析（ETA）



誘因事象	起因事象	火災検知器	フロン消化器	ｽﾌﾟﾘﾝｸﾗｰ	工場への影響	弁開操作
			成功		消火	
			0.8		1.44	
		成功		成功	消火・水浸し	
漏電		0.9		0.6	0.216	
0.7 回/年			失敗			
タバコ	火災発生		0.2			成功
1.2 回/年	2 回/年			失敗	全焼	0.5
雷				0.4	0.144	
0.1 回/年						
		失敗			全焼	失敗
		0.1			0.2	0.5
						有毒ｶﾞｽ放出頻度
			合計全焼頻度		0.344 回/年	0.172 回/年

Discussion：
安全性向上策を提案してください

微生物を扱う実験室

BSL1 （個体および地域社会へのリスクは無い、ないし低い）
ヒトや動物に疾患を起す可能性の無い微生物。（乳酸菌、黒カビ）

BSL2 （個体へのリスクが中等度、地域社会へのリスクは低い）
ヒトや動物に疾患を起す可能性はあるが実験室職員、地域社会、家畜、環境にとって重大な災害となる可能性のない病原体。実験室での曝露は、重篤な感染を起す可能性はあるが、有効な治療法や予防法が利用でき、感染が拡散するリスクは限られる。（大腸菌、ボツリヌス菌）

基本実験室

BSL3 （個体へのリスクが高い、地域社会へのリスクは低い）
通常、ヒトや動物に重篤な疾患を起すが、通常の条件下では感染は個体から他の個体への拡散は起こらない病原体。有効な治療法や予防法が利用できる。

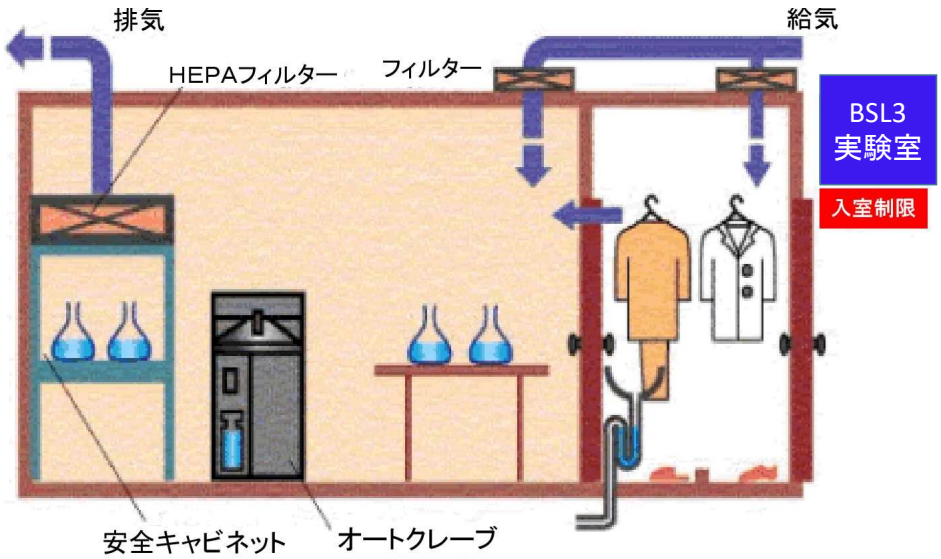
封じ込め実験室

BSL4 （個体および地域社会へのリスクが高い）
通常、ヒトや動物に重篤な疾患を起し、感染した個体から他の個体に、直接または間接的に容易に伝播され得る病原体。通常、有効な治療法や予防法が利用できない。

高度封じ込め実験室

BSL3を扱う実験施設

BSL3:　重篤な病気を起こすが、普通ヒトからヒトへの伝染はない。有効な治療法・予防法がある。炭そ菌、結核菌、黄熱ウイルス、狂犬病ウイルスなど

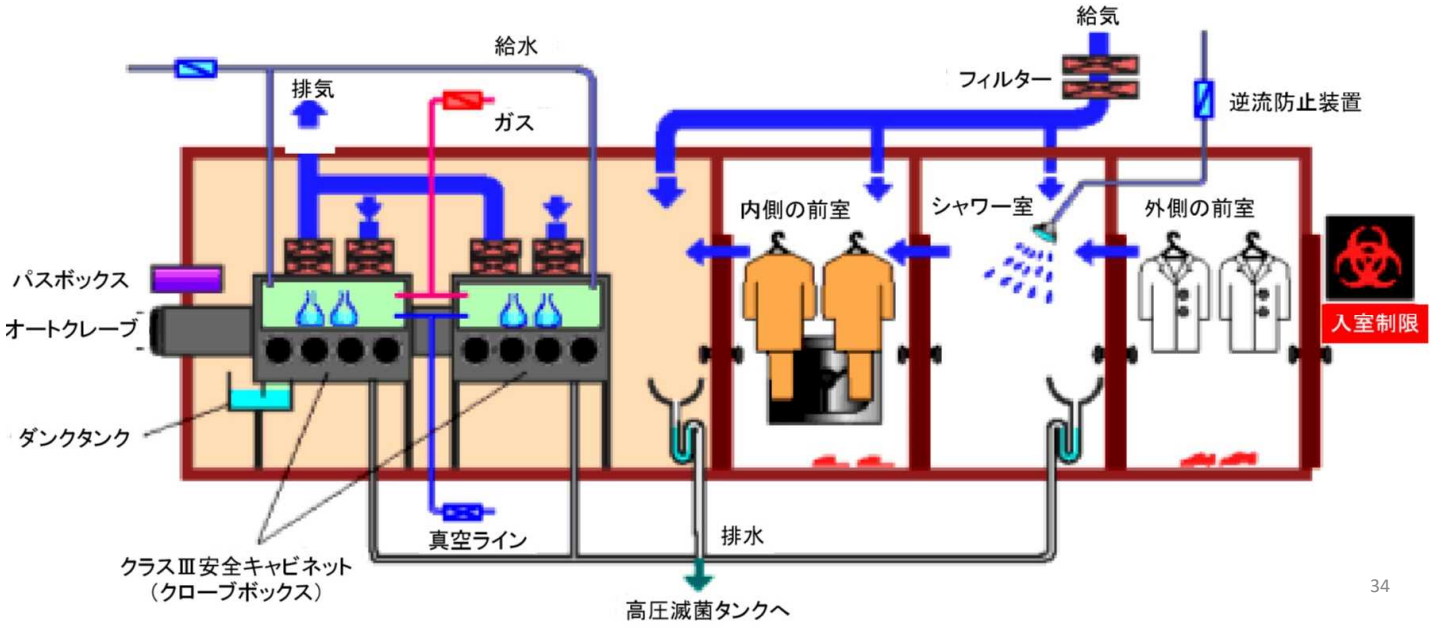


出典：国立医薬品食品衛生研究所HP

1. 安全キャビネットの設置
2. オートクレーブの設置
3. 更衣用の前室の設置、前室の前後の扉は同時に開かない構造
4. 空気が前室から実験区域へ流れるように設計された排気換気装置の設置
5. 出口に足等で操作できる手洗器の設置
6. 床、壁、天井の表面は容易に洗浄等ができる構造、材質

Discussion:　BSL4を扱う実験施設？

BSL4:　容易にヒトからヒトへ直接・間接の感染を起こす。有効な治療法・予防法は確立されていない。エボラ出血熱ウィルス、黄熱病ウィルスなど



Force on Force:

あなたはルーブル美術館の警備主任
モナリザの絵を盗賊から守る方法？

あなたは世界的に有名な盗賊
モナリザの絵を盗む方法？